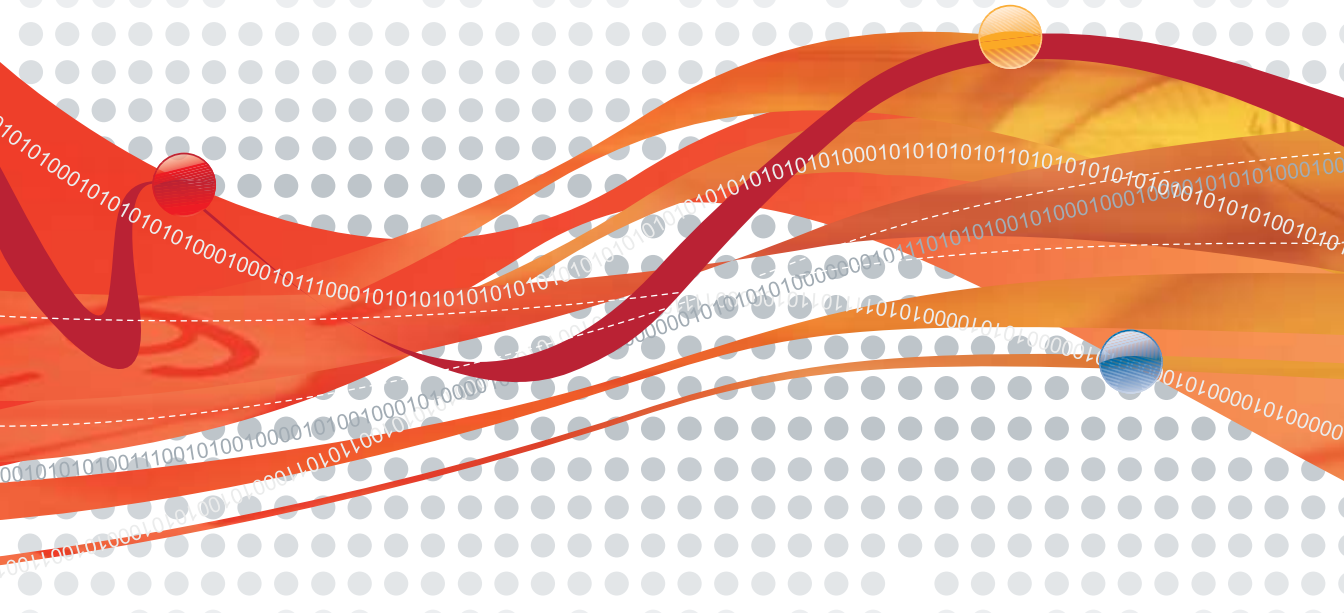
TREND MICRO™

InterScan™ Messaging Security Suite 7

Comprehensive threat protection at the Internet messaging gateway

for LINUX™

Administrator's Guide



Messaging Security

Document Part No. MSEM74063/90401

Release Date: June 2009

Patents Pending

The user documentation for Trend Micro™ InterScan™ Messaging Security Suite is intended to introduce the main features of the software and installation instructions for your production environment. You should read it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Chapter 1: Getting Started

Chapter 2: Configuring IMSS Settings

Chapter 3: Managing Policies

Chapter 4: Backing Up, Restoring, and Replicating Settings

Chapter 5: Monitoring the Network

Chapter 6: Using End User Quarantine

Chapter 7: Performing Administrative Tasks

Chapter 8: Troubleshooting, FAQ, and Support Information

Appendix A: IMSS Scripts

Appendix B: Default Directory Locations

Index

Preface

Welcome to the *Trend Micro™ InterScan™ Messaging Security Suite 7.1 Administrator's Guide.* This manual contains information on InterScan Messaging Security Suite™ (IMSS) features, system requirements, as well as instructions on configuring IMSS settings.

Refer to the *IMSS 7.1 Installation Guide* for information on how to install and upgrade IMSS.

Topics include:

Audience

The InterScan Messaging Security Suite documentation is written for IT administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP and POP3 protocols
- Message transfer agents (MTAs), such as Postfix or Microsoft™ Exchange
- LDAP
- Database management

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

InterScan Messaging Security Suite Documentation

The InterScan Messaging Security Suite (IMSS) documentation consists of the following:

- **Installation Guide:** Contains introductions to IMSS features, system requirements, and provides instructions on how to deploy and upgrade IMSS in various network environments.
- **Administrator's Guide:** Helps you get IMSS up and running with post-installation instructions on how to configure and administer IMSS.
- **Online Help:** Provides detailed instructions on each field and how to configure all features through the user interface. To access the online help, open the Web management console, then click the help icon ().
- **Readme Files:** Contain late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The *Installation Guide, Administrator's Guide* and *readme files* are available at:

http://www.trendmicro.com/download

Document Conventions

To help you locate and interpret information easily, the IMSS documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and other user interface items
Italics	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that must be avoided

Chapter 1

Getting Started

This chapter explains how to log on to the Web management console and provides instructions on what to do immediately after installation to get IMSS 7.1 up and running.

Topics include:

Opening the IMSS Web Management Console

You can view the IMSS management console using a Web browser from the server where you installed the program, or remotely across the network.

To view the console in a browser, type the following URL:

- https://<target server IP address>:8445

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

The default logon credentials are as follows:

- Administrator user name: **admin**
- Password: **imss7.1**

Type the logon credentials the first time you open the management console and click **Log On**.

Note: If you are using Internet Explorer 7.0 to access the Web management console, Internet Explorer will block the access and display a popup dialog box indicating that the certificate was issued from a different Web address. Add the Web console IP address to your **Trusted sites** list (**Internet Options > Security** in Internet Explorer) or ignore the message and click **Continue to this Web site** to proceed.

Tip: To prevent unauthorized access to the Web console, Trend Micro recommends changing the password regularly.

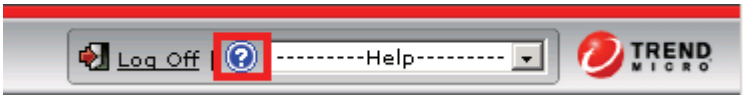
Using the Online Help

The IMSS Web management console comes with an Online Help that provides a description of each field on the user interface.

To access page-specific Online Help from the IMSS Web management console, click the Help icon located at the top right corner of the page.

To access the table of contents for the Online Help, click the Help icon next to the **Log Off** hyperlink on the right of the page header.

FIGURE 1-1. Table of Contents Access for Online Help



Viewing the Web Management Console Using Secure Socket Layer

The IMSS Web management console supports encrypted communication, using SSL. After installing IMSS, SSL communication should work because the installation contains a default certificate. Trend Micro suggests creating your own certificate to increase security.

If you want to use your own certificate, replace the following:

$IMSS_HOME/UI/tomcat/sslkey/.keystore

Creating an SSL Certificate

Do the following:

1. Create the Tomcat SSL certificate, for the IMSS Web console, as follows:

   $IMSS_HOME/UI/javaJRE/bin/keytool -genkey -alias tomcat -keyalg RSA -sigalg SHA1withRSA -keystore

   $IMSS_HOME/UI/tomcat/sslkey/.keystore -validity 3652

   For more details on SSL configuration in Tomcat, visit:

http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html

2. Create the Apache SSL certificate, for the EUQ Web console, as follows:

   a. Generate a Private Key and Certificate Signing Request (CSR)

   ```
   openssl req -new > new.cert.csr
   ```

   b. Remove pass-phrase from the key

   ```
   openssl rsa -in privkey.pem -out new.cert.key
   ```

   c. Generate a Self-Signed Certificate

   ```
   openssl x509 -in new.cert.csr -out new.cert.cert -req
   -signkey new.cert.key -days 3652 -sha1
   ```

   d. Copy the certificate and key to the Apache path

   ```
   cp new.cert.cert
   $IMSS_HOME/UI/apache/conf/ssl.crt/server.crt
   cp new.cert.key
   $IMSS_HOME/UI/apache/conf/ssl.key/server.key
   ```

Performing Basic Configuration with the Configuration Wizard

IMSS provides a configuration wizard to help you configure the basic settings required to get IMSS up and running.

The configuration wizard guides you through steps of configuring the following settings:

Step 1: Configuring Notification Settings

Step 2: Configuring the Update Source

Step 3: Configuring LDAP Settings

Step 4: Configuring Internal Addresses

Step 5: Configuring Control Manager Server Settings

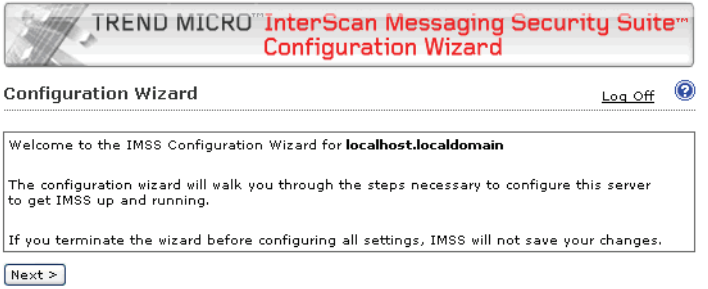
Step 6: Configuring Product Settings

Step 7: Verifying Settings Summary

Accessing the Configuration Wizard

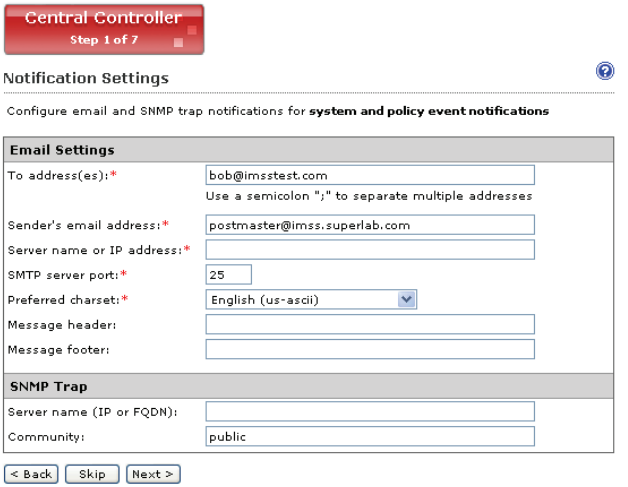
Access the wizard using one of the following methods:

- Log on to the Web management console and make sure the **Open Configuration Wizard** is selected on the log on screen, and then log on. The wizard opens.
- If you are already logged on to the Web management console, choose **Administration > IMSS Configuration > Configuration Wizard**. The wizard opens in a new window.



Step 1: Configuring Notification Settings

1. Click **Next**. The **Notification Settings** screen appears.

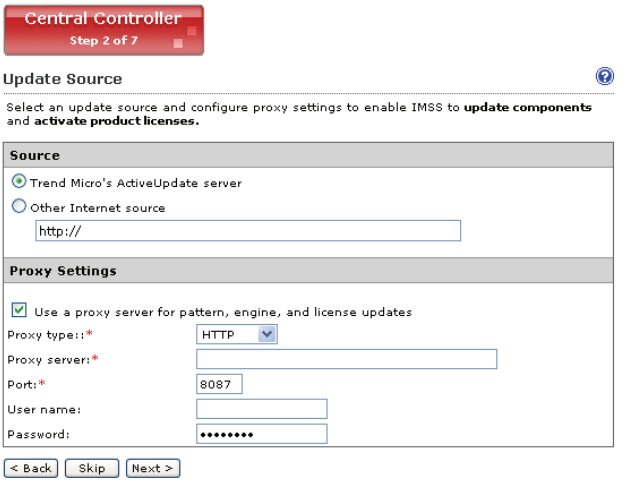


2. Configure the following notification settings, which IMSS will use for all default system and policy event notifications:
   - **Email Settings:** Type the sender and receiver addresses, the name of the server that IMSS delivers mail to, the SMTP server port, the language character set, and any additional headers or footers to add to the message.

- **SNMP Trap:** If you have an SNMP server on your network, type the server name and the community name.

Step 2: Configuring the Update Source

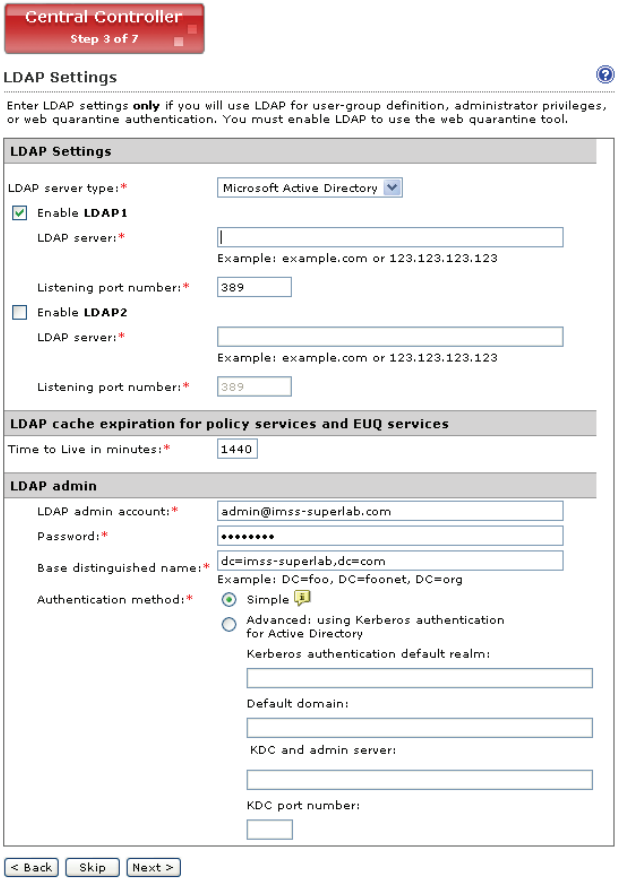
1. Click **Next**. The **Update Source** screen appears.



2. Configure the following update settings, which will determine from where IMSS will receive its component updates and through which proxy (if any) IMSS needs to connect to access the Internet:
   - **Source:** Click **Trend Micro ActiveUpdate (AU) server** to receive updates directly from Trend Micro. Alternatively, click **Other Internet source** and type the URL of the update source that will check the Trend Micro AU server for updates. You can specify an update source of your choice or type the URL of your Control Manager server, if applicable.
   - **Proxy Settings:** Select the **Use proxy server** check box and configure the proxy type, server name, port, user name, and passwords.

Step 3: Configuring LDAP Settings

1. Click **Next**. The **LDAP Settings** screen appears.



2. Complete the following to enable LDAP settings:
   a. For **LDAP server type**, select one of the following:
      - **Microsoft Active Directory**
      - **Domino**

- **Sun iPlanet Directory**

b. To enable one or both LDAP servers, select the check boxes next to **Enable LDAP 1** or **Enable LDAP 2**.

c. Type the names of the LDAP servers and the port numbers they listen on.

d. Under **LDAP Cache Expiration for Policy Services and EUQ services**, type a number that represents the time to live next to the **TTL in minutes** field.

e. Under **LDAP Admin**, type the administrator account, its corresponding password, and the base-distinguished name. See *Table 1-1* for a guide on what to specify for the LDAP admin settings.

TABLE 1-1. LDAP admin settings

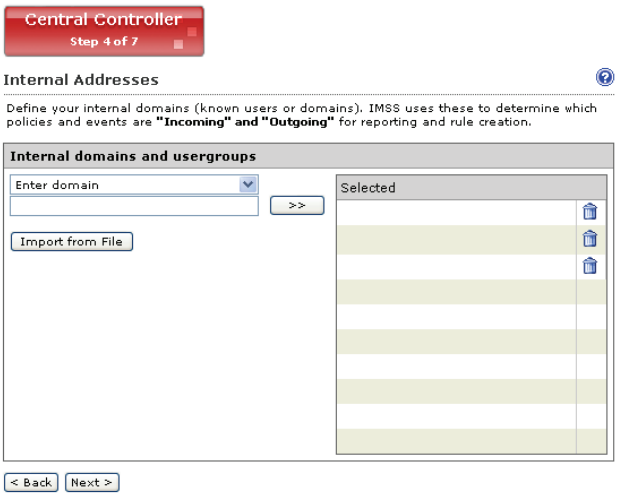
LDAP SERVER	LDAP ADMIN ACCOUNT (EXAMPLES)	BASE DISTINGUISHED NAME (EXAMPLES)	AUTHENTICATION METHOD
Active Directory	• Without Kerberos: user1@imsst-est.com (UPN) or imsstest\user1 • With Kerberos: user1@imsst-est.com	dc=imsstest, dc=com	• Simple • Advanced (with Kerberos)
Domino	user1/imsstest	Not applicable	Simple
Sun iPlanet Directory	uid=user1, ou=people, dc=imsstest, dc=com	dc=imsstest, dc=com	Simple

f. For **Authentication method**, click **Simple** or **Advanced** authentication. For Active Directory advanced authentication, configure the Kerberos authentication default realm, Default domain, KDC and admin server, and KDC port number.

Note: Specify LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or Web quarantine authentication. You must enable LDAP to use End-User Quarantine.

Step 4: Configuring Internal Addresses

1. Click **Next**. The **Internal Addresses** screen appears.



IMSS uses the internal addresses to determine whether a policy or an event is inbound or outbound.

- If you are configuring a rule for outgoing messages, the internal address list applies to the senders.
- If you are configuring a rule for incoming messages, the internal address list applies to the recipients.

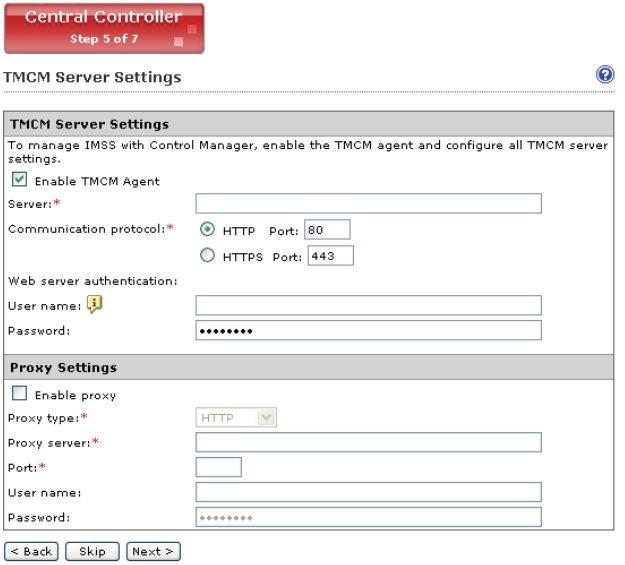
2. To define internal domains and user groups, do one of the following:
   - Select **Enter domain** from the drop-down list, type the domain in the text box, and then click **>>**.

- Select **Search for LDAP groups** from the drop-down list. A screen for selecting the LDAP groups appears. Type an LDAP group name to search in the text box and click **Search**. The search result appears in the list box. To add it to the **Selected** list, click **>>**.
- Click the **Import** button to import a text file containing a list of predefined domains.

Note: IMSS can only import a domain list from a text file (.txt). Ensure that the text file contains only one domain per line. You can also use wildcard characters to specify the domain. For example, ***.com** or ***.example.com**.

Step 5: Configuring Control Manager Server Settings

1. Click **Next**. The **TMCM Server Settings** screen appears.



2. If you will use Control Manager to manage IMSS, do the following:
   a. Select **Enable TMCM Agent** (installed with IMSS by default).

b. Next to **Server**, type the TMCM IP address or FQDN.

c. Next to **Communication protocol**, select **HTTP** or **HTTPS** and type the corresponding port number. The default port number for HTTP access is 80, and the default port number for HTTPS is 443.

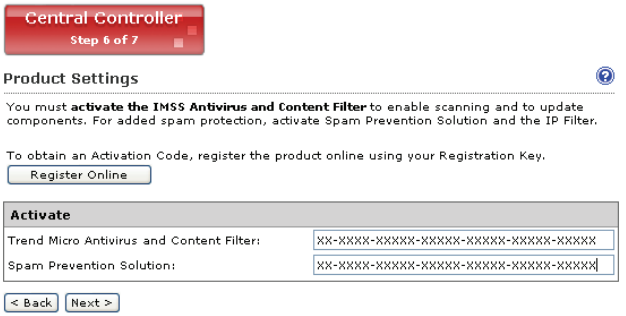
d. Under **Web server authentication**, type the user name and password for the Web server if it requires authentication.

e. If a proxy server is between IMSS and Control Manager, select **Enable proxy**.

f. Type the proxy server port number, user name, and password.

Step 6: Configuring Product Settings

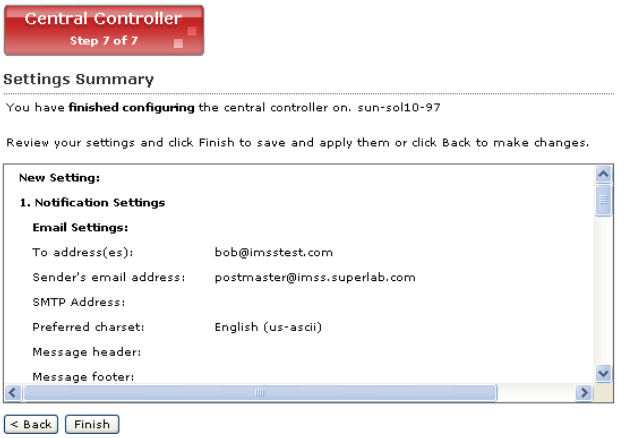
1. Click **Next**. The **Product Settings** screen appears. Activate the Antivirus and Content Filter to enable scanning and security updates. To obtain an Activation Code, register the product online using the supplied Registration Key.



2. Type the Activation Codes for the products you want to activate. If you do not have an Activation Code, click **Register Online** and follow the directions at the Trend Micro Registration Web site.

Step 7: Verifying Settings Summary

1. Click **Next**. A **Settings Summary** screen appears.



2. If your settings are correct, click **Finish**.

   To modify any of your settings, click **Back** and keep moving through the screens until your settings are complete.

Changing the Web Console Password

Trend Micro recommends periodically changing the password you use to access the Web management console.

To change the Web management console password:

1. Choose **Administration > Password**.
2. Type the current password, the new password, and the new password confirmation.

   The password must be between 4 and 32 alphanumeric characters.
3. Click **Save**.

WARNING! **If you are still using the default administration password, Trend Micro strongly recommends that you change the password immediately.**

Updating Scan Engine and Pattern Files

To ensure that your network is constantly protected against the latest malware, ensure that you update IMSS components such as the scan engine and virus pattern files on a regular basis. You can choose to perform a manual or scheduled update of the components.

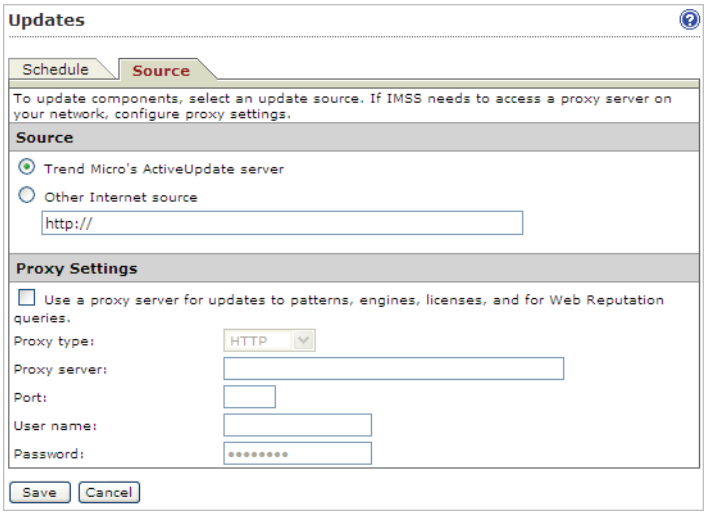
Specifying an Update Source

Before you can update the IMSS scan engine and pattern files, specify the update source. By default, IMSS downloads components from the Trend Micro ActiveUpdate server, which is the only source for up-to-date components. However, if you are using Trend Micro Control Manager to manage IMSS, you can update the components from the Control Manager server.

If you did not specify the update source when configuring IMSS using the Configuration Wizard, provide the update source and/or any proxy settings.

To specify an update source:

1. Choose **Administration** > **Updates** from the menu. The Updates screen appears.
2. Click the **Source** tab.



3. Under **Source**, select one of the following:
   - **Trend Micro ActiveUpdate server:** The default source for up-to-date components.
   - **Other Internet source:** Type the URL or IP address of the Control Manager server or other update source.
4. If the connection to ActiveUpdate, Product Registration Server, and Web reputation servers must pass through a proxy server, select **Use a proxy server for updates to patterns, engines, licenses, and for Web Reputation queries.** and configure the following:
   - **Proxy type:** Select **HTTP**, **SOCKS4**, or **SOCKS5**.
   - **Proxy server:** Type the host name or IP address of the proxy server.
   - **Port:** Type the port the proxy server uses to connect to the Internet.
   - **User name:** Type the username you need for administrative access to the proxy server.
   - **Password:** Type the corresponding password.
5. Click **Save**.

   If you are using the Configuration Wizard, click **Next**.

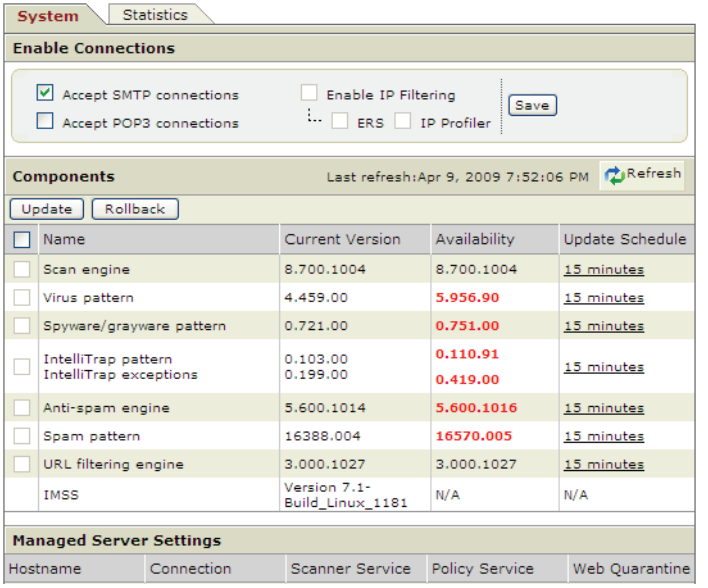
Performing a Manual Update

You should perform a manual update of IMSS components under the following circumstances:

- If you have just installed or upgraded IMSS.
- If you suspect that your network's security is compromised by new malware and would like to update the components immediately.

To perform a manual update:

1. Click **Summary** from the menu. The Summary screen appears with the System tab selected by default.



2. Under **Components**, verify the version numbers of the antivirus, anti-spyware, and anti-spam components that IMSS uses to protect your network.
3. To update all components, select the first check box on the column header next to the **Name** field. Otherwise, to update specific component(s), select the check box next to the desired component.
4. Click **Update**.

Rolling Back a Component Update

If you encounter any system issues after updating IMSS components, you can roll back to the previous version.

To roll back a component update:

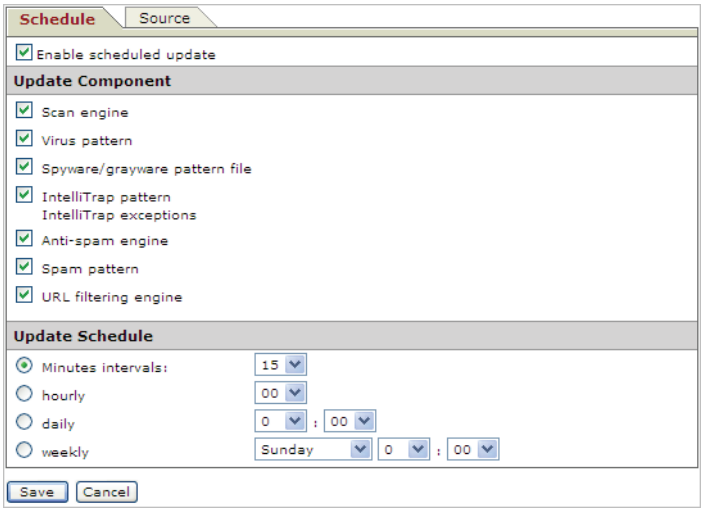
1. Choose **Summary** from the menu. The Summary screen appears with the System tab selected by default.
2. To roll back all components to the previous versions, select the first check box on the column header next to the **Name** field. Otherwise, to roll back specific component(s), select the check box next to the desired component.
3. Click the **Rollback** button.

Configuring Scheduled Update

If you forget to regularly download antivirus and anti-spam components, your network will be at risk from Internet threats. To automate the update process, configure an update schedule on this screen. If your network has limited Internet bandwidth, schedule updates during off-peak hours.

To configure a scheduled update:

1. Click **Administration** > **Updates** from the menu. The Updates screen appears with the Schedule tab selected by default.



2. Select the **Enable Scheduled Update** check box.
3. Under **Update Component**, select the components to update. Trend Micro recommends updating all components.
4. Under **Update Schedule**, select the update frequency:
   - **Minute intervals:** Updates every { } minutes per hour. Select the minute interval. For example, if you select 15, the update is triggered four times an hour: at 00, 15, 30, 45 minutes. If you select 30, the update will be triggered twice an hour: at 00 and 30 minutes.
   - **Hourly at minute:** Updates every hour at { } minutes. Select the number of minutes after the hour. For example, if you select 15, the update is triggered at 15 minutes after the hour, every hour.
   - **Daily at time:** Updates every day at the time you choose. Select the time of day.
   - **Weekly at day and time:** Updates once a week at the specified day and time. Select a day of the week and the time of day.
5. Click **Save**.

IMSS Services

The scanner and policy services must be started to start protecting your network using IMSS. You can, however, choose whether to install or start the EUQ service.

- **Scanner Services:** Performs scanning of SMTP/POP3 traffic.
- **Policy Services:** Acts as a remote store of rules for the scanner services to enhance rule lookups.
- **EUQ Services:** Hosts a Web-based console to enable end-users to view, delete and release spam messages addressed to them.

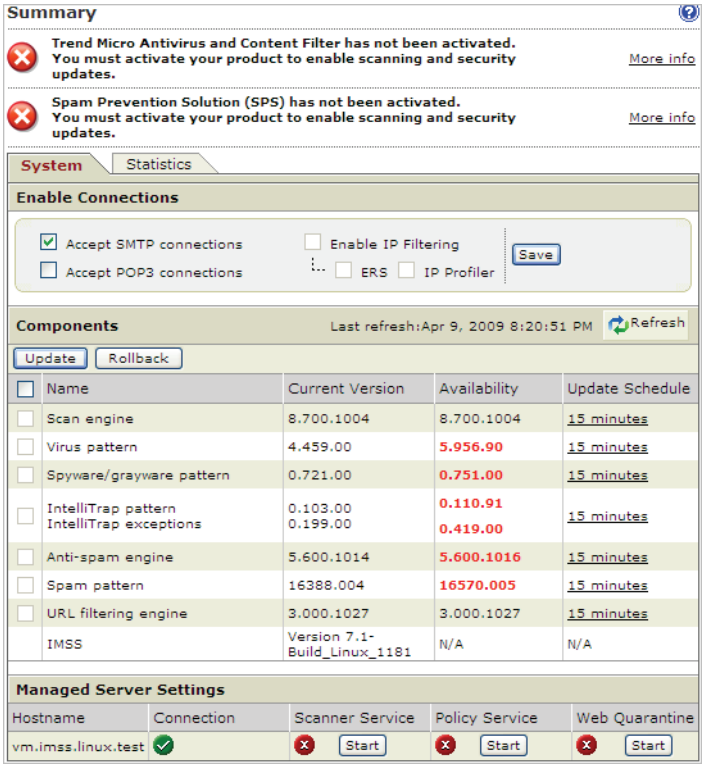
For more information on these services, refer to the IMSS Installation Guide.

Starting or Stopping Services

After you have successfully installed IMSS and configured the various settings, start the services to begin scanning for malware and other threats. Likewise, you may need to stop IMSS services prior to performing an upgrade or backup function.

To start or stop IMSS services:

1. Choose **Summary** from the menu. The Summary screen appears with the default System tab selected.



2. Under the Server Settings section, click the **Start** or **Stop** button for the service(s) that you would like to start or stop.

Opening the End-User Quarantine Console

Before you can access the EUQ Web console, ensure that you have done the following:

1. Configured the LDAP settings. See Step 3: Configuring LDAP Settings on page 1-8.
2. Enabled User Quarantine Access. See Configuring User Quarantine Access on page 5-35.

You can view the EUQ Web console from the computer where the program was installed or remotely across the network.

To view the console from another computer on the network, type the following URLs in an Internet browser:

- Primary EUQ service: `https://<target server IP address>:8447`
- Secondary EUQ service: `https://<target server IP address>:8446`

WARNING! **To successfully access all Web consoles on secondary EUQ services, you must synchronize the system time of all EUQ services on your network.**

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

Logon Name Format

The format of the user logon name for accessing the EUQ Web console differs according to the LDAP server type you have selected when configuring LDAP settings. Following are some examples of the logon name format for the three (3) types of supported LDAP servers:

- **Microsoft Active Directory**
  - Without Kerberos: `user1@imsstest.com (UPN) or imsstest\user1`
  - With Kerberos: `user1@imsstest.com`
- **Domino:** `user1/imsstest`
- **Sun iPlanet Directory:** `uid=user1, ou=people, dc=imsstest, dc=com`

Chapter 2

Configuring IMSS Settings

This chapter provides general descriptions on the various configuration tasks that you need to perform to get IMSS up and running. For further details, refer to the Online Help accessible from the Web management console.

IP Filtering Service

The IP Filtering service has two individual components: Email Reputation Service (ERS) and IP Profiler.

- Email Reputation Service (ERS) filters spam senders at the connection layer.
- IP Profiler helps protect the mail server from attacks with smart profiles (SMTP) Intrusion Detection Service (IDS).

Tip: Trend Micro recommends deploying IP Filtering as the first line of defense in your messaging infrastructure.

Although most email messaging systems have a multi-layer structure that often includes some pre-existing IP blocking, spam filtering, and virus filtering, Trend Micro recommends completely removing other IP blocking techniques from the messaging environment. IP Filtering should act as the precursor to any application filtering you might use.

Using Email Reputation Services

Trend Micro maintains a list of IP addresses belonging to known spam senders in a central database. Email Reputation Services (ERS) filters spam by blocking the IP addresses stored in this database.

Using the SPS Activation Code

IP Filtering Service, which includes ERS and IP Profiler, uses the same license as Spam Prevention Solution (SPS). If you purchase the full SPS service package, you will receive a Registration Key that will allow you to create a customer account with Trend Micro. Upon completion of the registration process, you will receive your Activation Code.

The Activation Code enables you to access the level of services according to your registration. When you activate SPS, the licensing information for IP Filtering will then appear.

For details on configuring ERS, see Configuring IP Filtering on page 2-8.

Preparing Your Message Transfer Agent for Use With Email Reputation Services

Configure your MTA to perform the appropriate DNS queries for the type of Email Reputation Service to which you subscribed.

- **ERS Standard:** Blocks connections with a 550 level error code ("connection refused"). The MTA returns this error code to the server initiating the connection because the IP address is in the Standard Reputation database as a known spammer.
- **ERS Advanced:** Configure the MTA to make two DNS queries. If the MTA does not receive a response from the first query to the standard reputation database, it makes a second query to the dynamic reputation database. The MTA should return a temporarily deny connection 450 level error code ("server temporarily unavailable, please retry") when a response is received from this database.

Legitimate email servers with compromised hosts temporarily sending spam may be listed in the dynamic reputation database. If the connection request is from a legitimate email server, it will re-queue and try sending the message later. This process will cause a short delay in mail delivery until the listing expires but will not permanently block the email.

Some servers may have additional options for handling questionable IP connections. These options include throttling or routing messages for more detailed scanning.

You can find instructions for configuring the MTA or firewall on the Trend Micro Web site:

https://tmspn.securecloud.com/

These instructions have been provided by the vendor or manufacturer of the product (MTA or firewall). Refer to your product manuals and/or technical support organization for detailed configuration and setup options.

Note: Insert your Activation Code to replace the instructional text example; do not include any dashes.

Using the ERS Management Console

Log on to the Email Reputation Services management console to access global spam information, view reports, create or manage ERS settings, and perform administrative tasks.

This section includes basic instructions for using the ERS console. For detailed instructions on configuring the settings for each screen, see the ERS console Online Help. Click the help icon in the upper right corner of any help screen to access the Online Help.

To open the ERS Management Console:

1. Open a Web browser and type the following address:

   https://tmspn.securecloud.com/

2. Log on using your Email Reputation Services user name and password. The Smart Protection Network portal opens with the **Email** tab selected and the **General** screen displaying.
3. Select **Global Spam Statistics** from the menu. The Global Spam Statistics screen appears.

   The Global Spam Statistics screen ranks ISPs based on the amount of spam they receive. The ISP Spam list displays the total spam volume from the top 100 ISPs for a specific week. The networks that are producing the most spam are ranked at the top. The ranking of the ISPs changes on a daily basis. The ISP Spam list displays the following:

TABLE 2-1. ISP Spam List

COLUMN	DESCRIPTION
Rank This Week	Displays the global rank for this week in terms of total spam volume.
Rank Last Week	Displays the global rank for the previous week in terms of total spam volume.

TABLE 2-1. ISP Spam List

COLUMN	DESCRIPTION
ASN	The Autonomous System Number (ASN) is a globally unique identifier for a group of IP networks having a single, clearly defined routing policy that is run by one or more network operators.
ISP Name	The registered name for a particular ASN. Some ISPs may have multiple ASNs and therefore appear more than once in the table.
Spam Volume (24 hours)	The estimated total spam that has been sent during the previous 24 hours. This total is updated every hour.
Botnet Activity	An indication of how active botnets are for your email servers. Botnets are groups of infected computers that are controlled by a spammer from a central location and are the largest source of spam on the Internet today. This number indicates the percentage change in the number of bots from the previous hour. To see botnet activity, you must add your email servers to the Valid Mail Servers list.

4. Click **News**. The News screen appears.

   The News screen displays breaking news about new spam and new features available for Email Reputation Services. Click the following tabs for information:

   - **Spam News:** Provides a brief overview and discussion of current spamming tactics and the implications for organizations. It also describes how new tactics are deployed, how they evade Trend Micro systems, and what Trend Micro is doing to respond to these new threats.
   - **Release News:** Provides a brief overview of new features available in Email Reputation Services

5. To view reports that summarize the activity between the MTA and the Email Reputation Services database servers, do the following:

   a. Select **Report** from the menu. A sub-menu appears.

b. Click one of the following:

TABLE 2-2. Report Types

REPORT	DESCRIPTION
Percentage Queries	The report shows the percentage of queries that returned an IP address match, which indicates that a sender trying to establish a connection with your email server is a known spammer. The reports are based on connections, not individual spam messages.
Queries per Hour	The report shows how many times your email server queried the reputation database.
Queries per Day	The report shows how many times per day your email server queried the reputation database.
Botnet Report	The report provides a quick summary of the last seven days of spam activity originating from the servers that you listed as valid mail servers. If there was any spam activity in the last seven days for any of the IP addresses that you specified, a red robot icon appears.

6. To manage protection provided by ERS settings:

a. Select **Policy** from the menu. A sub-menu appears.

b. Click one of the following:

TABLE 2-3. Policy Settings

POLICY	DESCRIPTION
Settings	Configure the Approved and Blocked senders lists. You can define your lists by individual IP address and CIDR by Country, or by ISP. • **Approved Sender:** Allows messages from the approved senders to bypass IP-level filtering. The Approved Sender lists are not applied to your MTA, but you can set up additional approved or blocked senders lists or do additional filtering at your MTA. • **Blocked Sender:** Instructs ERS to always block email messages from certain countries, ISPs, and IP addresses.
New ISP Request	Trend Micro welcomes suggestions from customers regarding other Internet Service Providers (ISPs) to be added to the service. Provide as much information about an ISP as you can. This helps Trend Micro to add the ISP to the service.
Reputation Settings	Configure ERS Standard and Advanced settings. Standard customers will see only the Enable Standard Settings section. Advanced customers will see both the Dynamic Settings and the Enable Standard Settings sections.

7. To change your password or Activation Code or to add your mail servers to ERS, choose **Administration** from the menu.

Configuring IP Filtering

To configure IP Filtering, perform the following steps:

Step 1. Enable ERS and IP Profiler

Step 2. Enable IP Profiler Rules

Step 3. Configure ERS

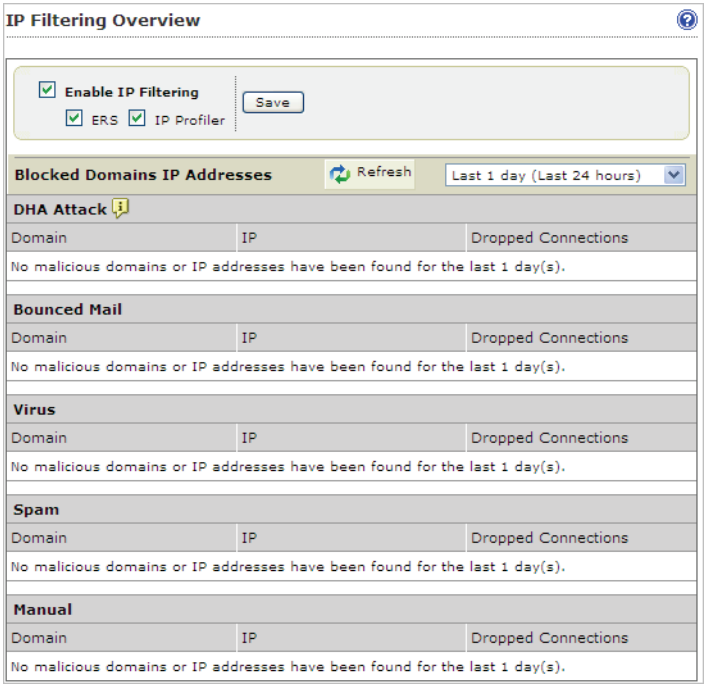
Step 4. Add IP Addresses to the Approved List

Step 5. Add IP Addresses to the Blocked List

Step 1: Enabling ERS and IP Profiler

To enable ERS and IP Profiler:

1. Choose **IP Filtering > Overview** from the menu. The IP Filtering Overview screen appears.



2. Select the **Enable IP Filtering** check box. This will select both the ERS and IP Profiler check boxes.
3. Clear the **ERS** or **IP Profiler** check box, if you do not require them.
4. Click **Save**.

Note: If you decide to disable IP filtering subsequently, uninstall ERS and IP Profiler manually. Disabling IP filtering from the Web management console only unregisters IP Profiler from IMSS but does not stop ERS and IP Profiler from running. For more information on uninstalling ERS and IP Profiler, see the *Uninstalling Email Reputation Services and IP Profiler* section of the *IMSS Installation Guide*.

Step 2: Enabling IP Profiler Rules

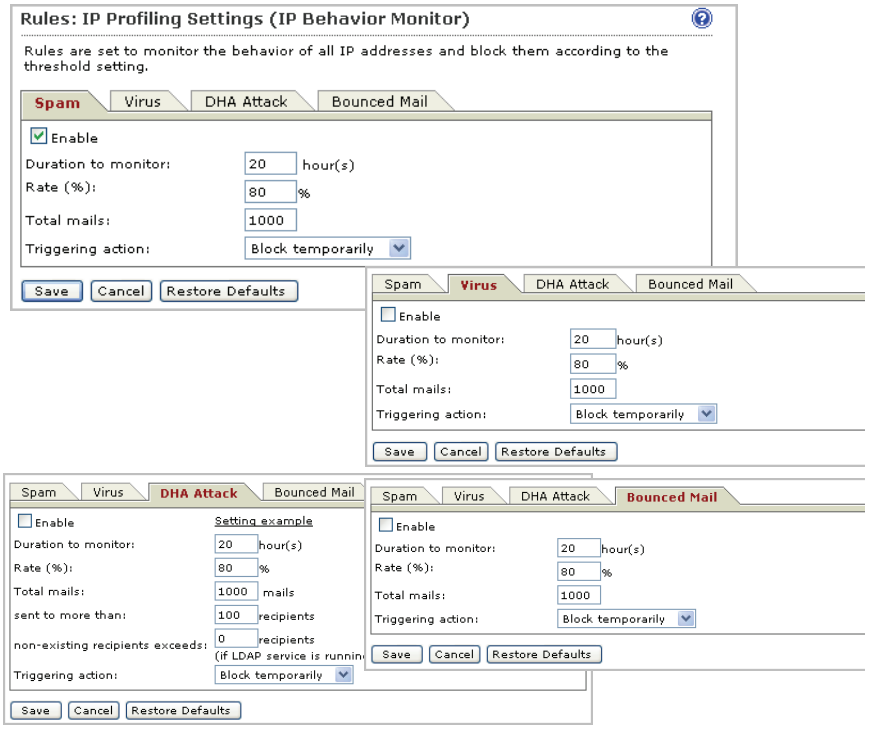
Rules are set to monitor the behavior of all IP addresses and block them according to the threshold setting. Rules can be set for the following:

- Spam
- Viruses
- DHS attacks
- Bounced mail

WARNING! **Before enabling IP Profiler Rules, add all of your email servers' IP addresses (that send outgoing email messages to IMSS) to the IP Filtering Approved List. To configure the IP Filtering Approved List, see** Step 4: Adding IP Addresses to the Approved List on page 2-20**.**

To specify IP filtering Spam Settings:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.



2. Click the **Spam** tab. The Spam screen appears.
3. Select the **Enable** check box to enable blocking of spam.
4. Specify a value for the following:
   - **Duration to monitor:** The number of hours that IMSS monitors email traffic to see if the percentage of spam email messages exceeds the **Threshold** you set.
   - **Rate (%):** Type the maximum number of allowable email messages with spam threats.

- **Total mails:** Type the total number of spam email messages out of which the threshold percentage is calculated.

  Consider the following example.

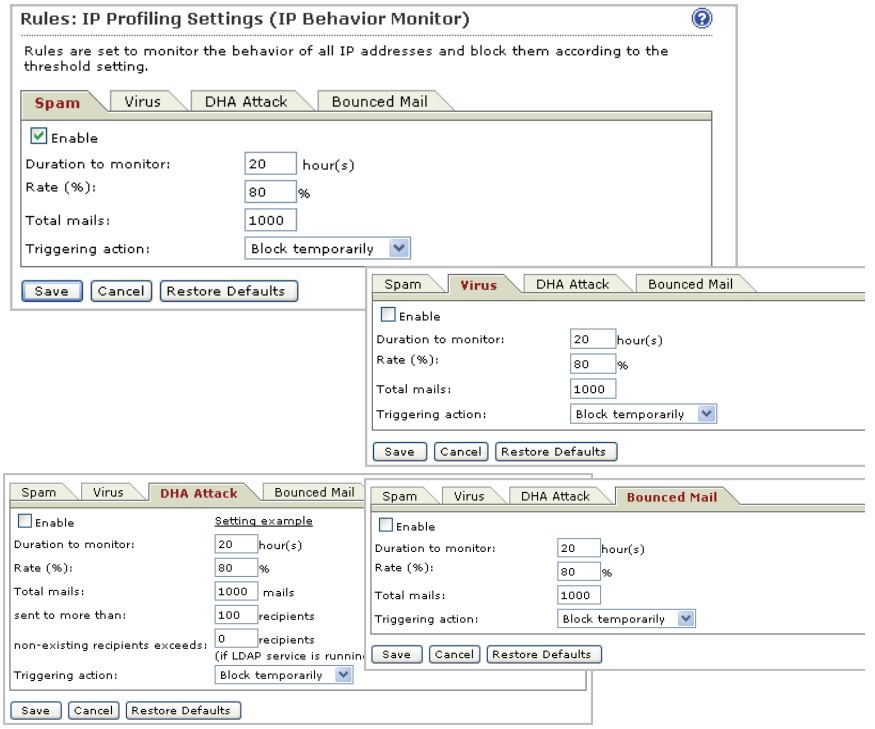
  Duration to monitor: 1 hour at a rate of 20 out of 100

  During each one-hour period that spam blocking is active, IMSS starts blocking IP addresses when more than 20% of the messages it receives contain spam and the total number of messages exceeds 100.

5. Next to **Triggering action**, select one of the following:
   - **Block temporarily:** Block email messages from the IP address and allow the upstream MTA to try again.
   - **Block permanently:** Never allow another email message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

To specify IP filtering Virus Settings:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.



2. Click the **Virus** tab. The Virus screen appears.
3. Select the **Enable** check box to enable blocking of virus threats.
4. Configure the following:
   - **Duration to monitor:** The number of hours that IMSS monitors email traffic to see if the percentage of email messages with virus threats exceeds the Threshold you set.
   - **Rate (%):** Type the maximum number of allowable email messages with virus threats (the numerator).

- **Total mails:** Type the total number of infected email messages out of which the threshold percentage is calculated (the denominator).

  Consider the following example.

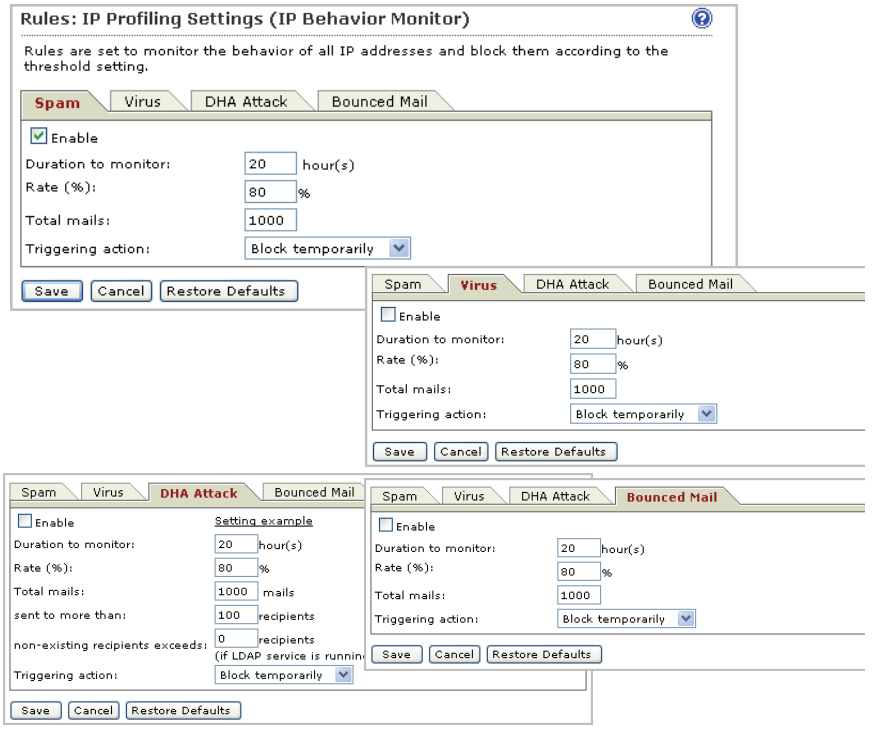
  Duration to monitor: 1 hour at a rate of 20 out of 100

  During each one-hour period that virus blocking is active, IMSS starts blocking IP addresses when more than 20% of the messages it receives contain virus threats and the total number of messages exceeds 100.

5. Next to **Triggering action**, select one of the following:
   - **Block temporarily:** Block email messages from the IP address and allow the upstream MTA to try again.
   - **Block permanently:** Never allow another email message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

To specify Directory Harvest Attack (DHA) Settings:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.



2. Click the **DHA Attack** tab. The DHA Attack screen appears.
3. Select the **Enable** check box to enable blocking of directory harvest attacks.
4. Configure the following:
   - **Duration to monitor:** The number of hours that IMSS monitors email traffic to see if the percentage of email messages signaling a DHA attack exceeds the Threshold you set.
   - **Rate (%):** Type the maximum number of allowable email messages with DHA threats (the numerator).

- **Total mails:** Type the total number of DHA email messages out of which the threshold percentage is calculated (the denominator).
- **Sent to more than:** Type the maximum number of recipients allowed for the threshold value.
- **Non-existing recipients exceeds:** Type the maximum number of non-existent recipients allowed for the threshold value. DHA attacks often include randomly generated email addresses in the receiver list.

Note: The LDAP service must be running to determine non-existing recipients.

Consider the following example.

Duration to monitor: 1 hour at a rate of 20 out of 100 sent to more than 10 recipients when the number of non-existing recipients exceeds 5.

During each one-hour period that DHA blocking is active, IMSS starts blocking IP addresses when it receives more than 20% of the messages that were sent to more than 10 recipients (with more than five of the recipients not in your organization) and the total number of messages exceeds 100.

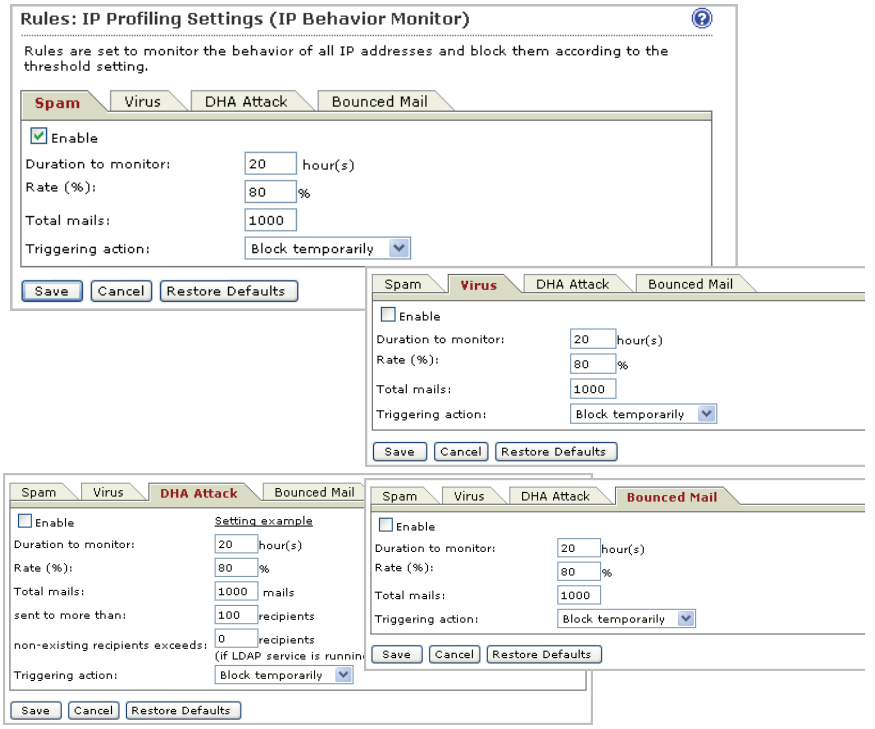
Tip: Technically, the LDAP server is not a must-have. The DHA rule of IMSS can also obtain the DHA results returned from Postfix, which in turn passes these results to FoxProxy through the LDAP server or other means. FoxProxy then analyzes the results to determine if they are DHA attacks.

LDAP server is only one of the means by which Postfix checks if a user's mailbox exists.

5. Next to **Triggering** action, select one of the following:
   - **Block temporarily:** Block email messages from the IP address and allow the upstream MTA to try again.
   - **Block permanently:** Never allow another email message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

To specify Bounced Mail Settings:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.



2. Click the **Bounced Mail** tab. The Bounced Mail screen appears.
3. Select the **Enable** check box to enable blocking of bounced mail.
4. Configure the following:
   - **Duration to monitor:** The number of hours that IMSS monitors email traffic to see if the percentage of email messages signaling bounced mail exceeds the Threshold you set.
   - **Rate (%):** Type the maximum number of allowable email messages signaling bounced mail (the numerator).

- **Total mails:** Type the total number of bounced email messages out of which the threshold percentage is calculated (the denominator).

  Consider the following example.

  Duration to monitor: 1 hour at a rate of 20 out of 100

  During each one-hour period that blocking for bounced mail is active, IMSS starts blocking IP addresses when more than 20% of the messages it receives are bounced messages and the total number of messages exceeds 100.

Note: The LDAP service must be running to check bounced mail.

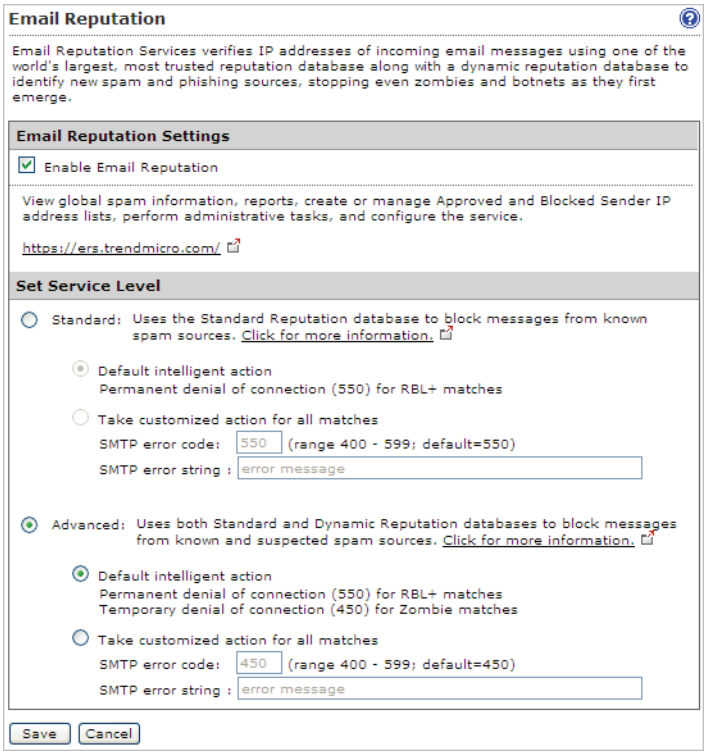
---

5. Next to **Triggering action**, select one of the following:
   - **Block temporarily:** Block email messages from the IP address and allow the upstream MTA to try again.
   - **Block permanently:** Never allow another email message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

Step 3: Configuring ERS

To configure ERS:

1. Choose **IP Filtering > ERS** from the menu. The ERS screen appears.



2. Select the **Enable ERS** check box.
3. Click a radio button next to one of the following, depending on your level of service, and configure the settings:

   Standard:

   - **Default intelligent action:** ERS permanently denies connection (550) for RBL+ matches.
   - **Take customized action for all matches**

- **SMTP error code:** Blocks any connections that have a certain SMTP code. Type an SMTP code.
- **SMTP error string:** Type the message associated with the SMTP error code.

Advanced:

- **Default intelligent action:** ERS permanently denies connection (550) for RBL+ matches and temporarily denies connection (450) for Zombie matches.
- **Take customized action for all matches**
  - **SMTP error code:** Blocks any connections that have a certain SMTP code. Type an SMTP code.
  - **SMTP error string:** Type the message associated with the SMTP error code.

Note: The above SMTP error code and error string will be sent to the upstream MTA that will then take the necessary preconfigured actions, such as recording the error code and error string in a log file.

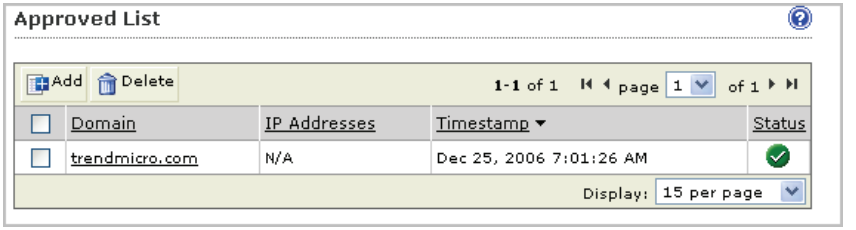
4. Click **Save**.

Step 4: Adding IP Addresses to the Approved List

IMSS does not filter IP addresses or domains that appear in the Approved List.

To add an IP address to the approved list:

1. Choose **IP Filtering > Approved List** from the menu. The Approved List screen appears.



2. Click **Add**. The Add IP/Domain to Approved List screen appears.

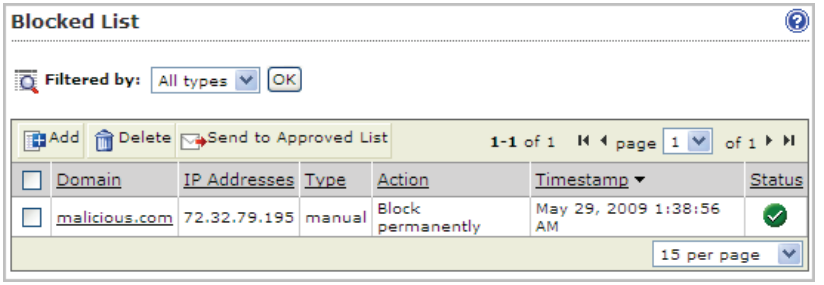
3. Select the **Enable** check box.
4. Type the domain or IP address that you would like to add to the Approved List.
5. Click **Save**. The domain or IP address appears in the Approved List.

Step 5: Adding IP Addresses to the Blocked List

IMSS blocks IP addresses that appear in the Blocked List.

To add an IP address to the Blocked List:

1. Choose **IP Filtering > Blocked List** from the menu. The Blocked List screen appears.



2. Click **Add**. The Add IP/Domain to Blocked List screen appears.

3. Select the **Enable** check box.
4. Type the domain or IP address.
5. Select **Block temporarily** or **Block permanently**.
6. Click **Save**. The domain or IP address is added to the blocked list.

Displaying Suspicious IP Addresses and Domains

IMSS creates log entries of the IP addresses or domains that have sent email messages violating scanning conditions, but are still not blocked because the total number of messages did not exceed the threshold you set for the given time period.

To display suspicious IP addresses and domains:

1. Click **IP Filtering > Suspicious IP/Domain**.
2. Choose from any of the following conditions:
   - Next to **Type**, select the check boxes next to the type of threat that the IP filter detected.
   - Next to **Dates**, select the date-time range within which IMSS blocked the sender.
   - If you know a specific IP address to query, type it next to **IP**.
   - To display the corresponding domain names of the IP addresses, select the **Show Domain names** check box.
   - Next to **Logs per page**, select the number of log entries to display on the screen at a time.
3. Click **Display Log**.
4. Perform any of the additional actions:

- To block an IP address temporarily, select the corresponding check box in the list, then click **Block Temporarily**.
- To block an IP address permanently, select the corresponding check box in the list, then click **Block Permanently**.
- To change the number of items that appears in the list at a time, select a new display value from the drop down box on the top of the table.
- To sort the table, click the column title.

Scanning SMTP Messages

IMSS supports three types of Message Transfer Agents (MTA). They are Postfix, Sendmail, and Qmail.

If you are using Postfix with IMSS and have deployed multiple scanner services, you can manage the SMTP routing settings for the scanner services centrally. From the IMSS Web management console, configure the SMTP settings and apply the same settings to all scanners.

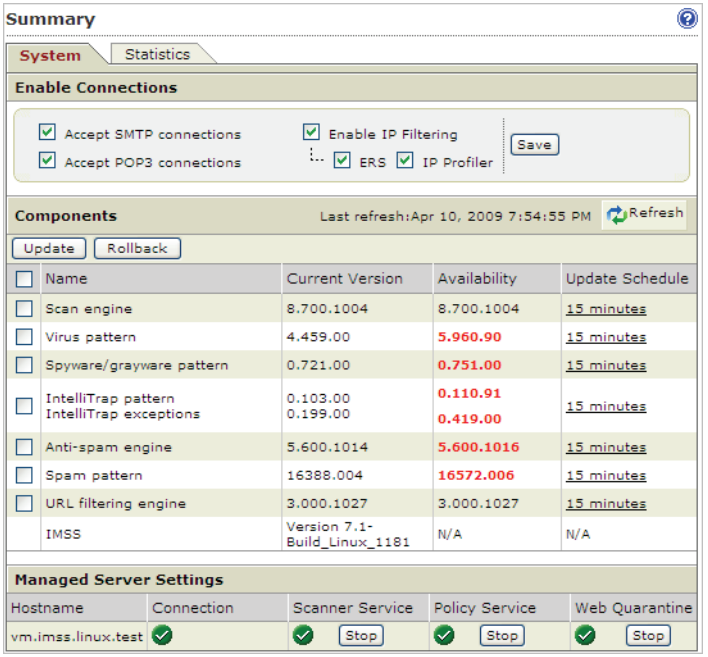
If you are using Sendmail or Qmail, you will need to manually configure the SMTP settings in the respective MTA configuration files. For details, see Preparing Message Transfer Agents section of the IMSS Installation Guide.

Enabling SMTP Connections

Before IMSS can start scanning incoming and outgoing traffic on your network, enable SMTP connections.

To enable SMTP connections:

1. Choose **Summary** from the menu. The System tab appears by default.



2. Select the check box next to **Accept SMTP connections**.
3. Click **Save**.

Configuring SMTP Routing

Configuring SMTP routing involves the following steps:

Step 1. Configure SMTP settings

Step 2. Configure Connections settings

Step 3. Configure Message Rule settings

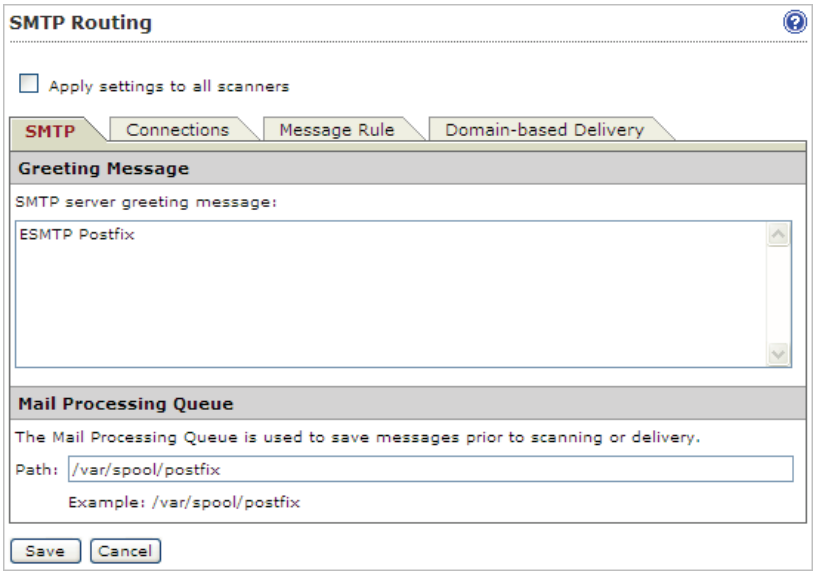
Step 4. Configure Domain-based Delivery settings

Configuring SMTP Settings

Use the SMTP screen to configure SMTP settings for the MTA, such as the SMTP greeting message and the location of the mail processing queue, where IMSS saves messages before it scans and delivers them.

To specify the SMTP settings:

1. Click **Administration > IMSS Configuration > SMTP Routing**. The SMTP Routing screen appears.



2. Select the **Apply settings to all scanner** check box.

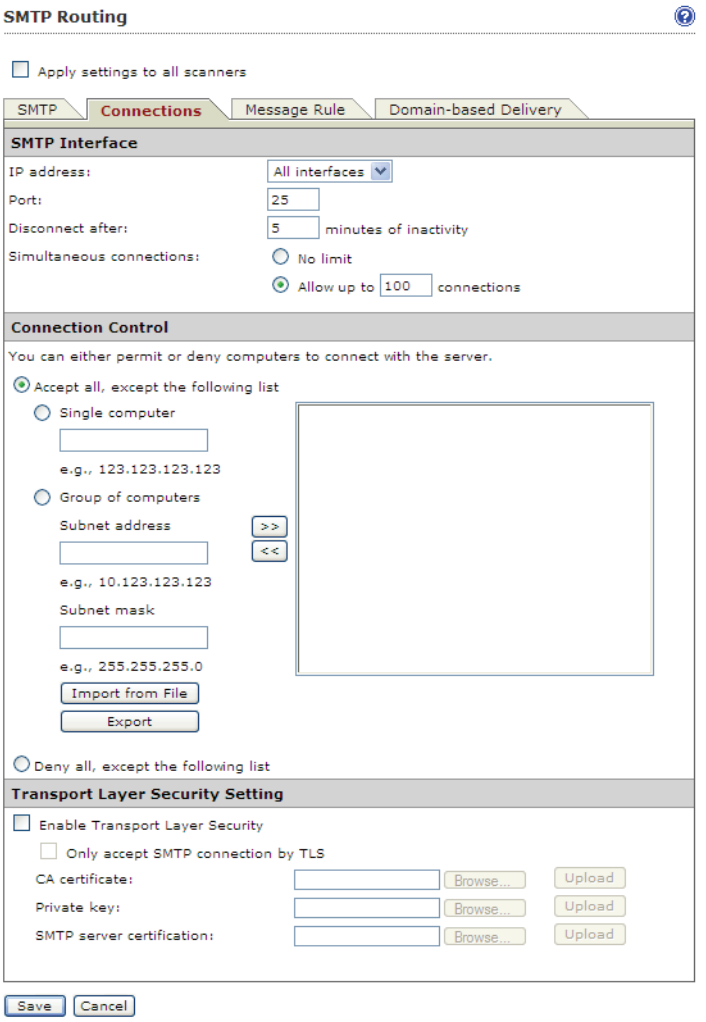
   This option applies all the settings configured in the SMTP, Connections, Message Rule and Domain-based Delivery tabs to all scanners connected to the same IMSS Administration database.

3. Specify SMTP server **Greeting Message** (displays when a session is created).
4. Specify the **Mail Processing Queue Path**.
5. Click **Save**.

Configuring Connections Settings

To specify the Connections settings:

1. Choose **Administration > IMSS Configuration > SMTP Routing** from the menu**.**
2. Click the **Connections** tab. The Connections screen appears.



3. Specify the **SMTP Interface** settings:
   - **IP address:** Select the interface that will connect with your SMTP server.
     - **127.0.0.1:** The SMTP server will only listen to the IP address on the local computer.

- **All interfaces:** If there are multiple IP addresses on this computer, the SMTP server will listen to any of the IP addresses available.

- **Port:** Type the listening port of the SMTP server.
- **Disconnect after { } minutes of inactivity:** Type a timeout value.
- **Simultaneous connections:** Click **No limit** or **Allow up to { } connections** and type the maximum number of connections.

4. Specify the **Connection Control** settings:
   - **Accept all, except the following list:** Configure the "deny list" using the following:
     - **Single computer:** Type an IP address, and then click **>>** to add it to the list.
     - **Group of computers:** Type a subnet address and mask, and then click **>>** to add the group to the list.
     - **Import from file:** Click to import a "deny list" from a file. The following shows sample content of an IP list text file:

       192.168.1.1

       192.168.2.0:255.255.255.0

       192.168.3.1:255.255.255.128

       192.168.4.100

       192.168.5.32:255.255.255.192
   - **Deny all, except the following list**: Configure the "permit list" using the following.
     - **Single computer:** Type an IP address, and then click **>>** to add it to the list.
     - **Group of computers:** Type a subnet address and mask, and then click **>>** to add the group to the list.
     - **Import from file:** Click to import a "permit list" from a file. The following shows sample content of an IP list text file:

       192.168.1.1

       192.168.3.1:255.255.255.128

       192.168.4.100

       192.168.5.32:255.255.255.192

5. Specify the **Transport Layer Security Settings**:
   a. Select **Enable Transport Layer Security**.

      This option allows the IMSS SMTP Server to provide Transport Layer Security (TLS) support to SMTP clients, but does not require that clients use TLS encryption to establish the connection.

   b. Select **Only accept SMTP connection by TLS** for IMSS to only accept secure incoming connections.

      This option enables the IMSS SMTP Server to accept messages only through a TLS connection.

   c. Click a **Browse** button next to one of the following:

      - **CA certificate:** A CA certificate is usually used for verifying SMTP clients. However, IMSS does not verify the client and only uses the CA certificate for enabling the TLS connection.

        Only upload this file if it is provided to you together with the public key. Otherwise, this file is not mandatory for enabling a TLS connection.

      - **Private key:** The SMTP client encrypts a random number using IMSS SMTP server's public key and an encryption key to generate the session keys.

        IMSS SMTP server then uses the private key to decrypt the random number in order to establish the secure connection.

        This key must be uploaded to enable a TLS connection.

      - **SMTP server certification:** The IMSS SMTP server's public key made available to the SMTP clients for generating the session keys.

        This key must be uploaded to enable a TLS connection.

   d. Click **Upload** to save the file on the IMSS server.

6. Click **Save**.

Configuring Message Rule Settings

To set limits on the email messages that IMSS can handle and to control email relay, configure all settings on the messages rules screen.

Email Relay

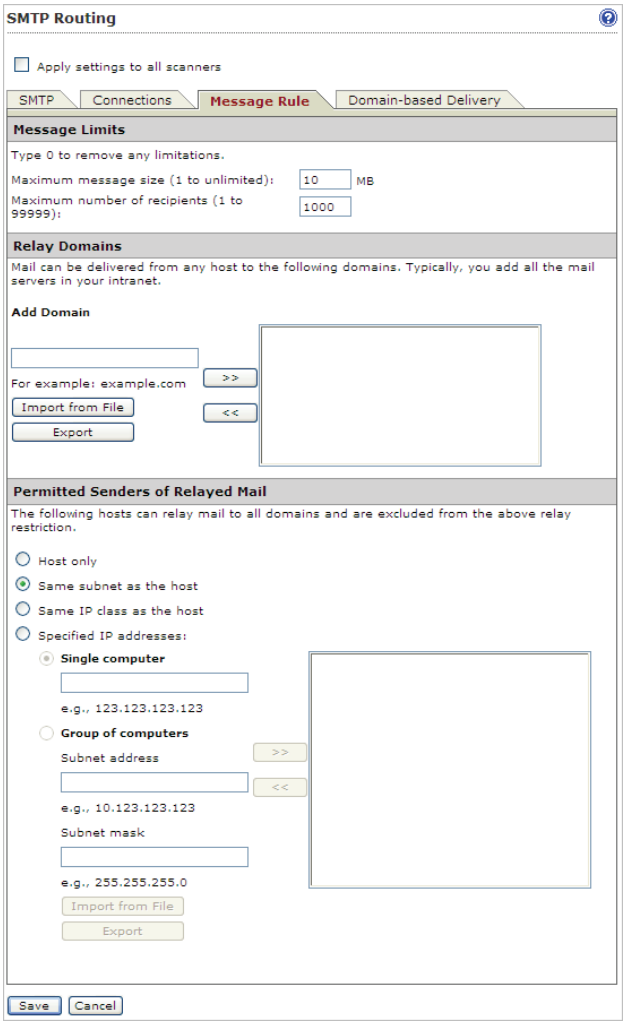
To prevent spammers from using the IMSS MTA as a relay for spam, configure relay control by adding the mail domains on your network to the Relay Domains list. When IMSS receives an email message, it looks at the final destination of the email and compares it to this list. IMSS discards the message under the following circumstances:

- The destination domain is not in this list
- The parent domain of the destination domain is not in this list
- The host is not on the **Permitted Senders of Relayed Mail** list

Relay domain settings are different from Domain-based delivery settings. For an explanation, see About Domain-Based Delivery on page 2-34.

To specify the Message Rules:

1. Choose **Administration > IMSS Configuration > SMTP Routing** from the menu.
2. Click the **Message Rule** tab. The Message Rule screen appears.



3. Specify the **Message Limits** settings:
   - **Maximum message size:** Type the number of megabytes.
   - **Maximum number of recipients:** Type the number of recipients from 1 to 99999.

4. Specify the **Relay Domains**. IMSS relays the messages to the listed domains.

   Tip: When importing, import both the exact domain and all sub-domains for best results.

   The following shows sample content of a domain list text file:

   - **domain.com**: Imports the exact domain
   - ***.domain.com**: Imports all sub-domains
   - **domain.org**: Imports the exact domain

   Note: The import file must be a text file containing one domain per line. You can use wildcards when specifying the domain.

5. Specify the **Permitted Senders of Relayed Mail**.
6. Click **Save**.

About Domain-Based Delivery

IMSS maintains a routing table based on the domain names of recipient email addresses. IMSS then uses this routing table to route emails (with matching recipient email addresses) to specified SMTP servers using domain-based delivery. Messages destined to all other domains will be routed based on the records in the Domain Name Server (DNS).

Relay Domains and Domain-Based Delivery

The domains you configure for relay domain settings (for SMTP Message Rules) are different from the domains you configure for domain-based delivery settings (for Domain-Based Delivery).

Relay domains: IMSS relays email messages that are sent only to the relay domains. For example, if the relay domains list includes only one domain, "domain.com", IMSS will relay only email messages that are sent to "domain.com".

Domain-based delivery domains: IMSS delivers email based on domain-based delivery. For example, if the delivery domains include "domain.com" and the associated SMTP server 10.10.10.10 on port 25, all email messages sent to "domain.com" will be delivered to the SMTP server 10.10.10.10 using port 25.

Configuring Domain-based Delivery Settings

Specify settings for the next stage of delivery. IMSS checks the recipient mail domain and sends the mail to the next SMTP host for the matched domain.

When importing a Domain-based Delivery list, provide one entry per line. Each entry consists of the following:

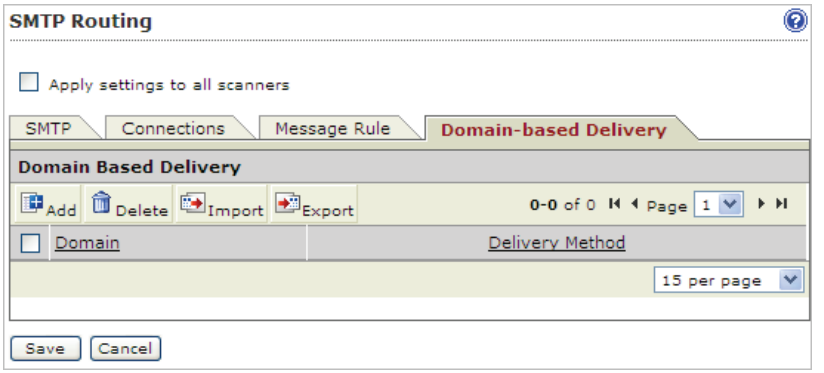
```
[domain name],[server name or IP address]:[port number]
```

For example, all of the following are valid entries:

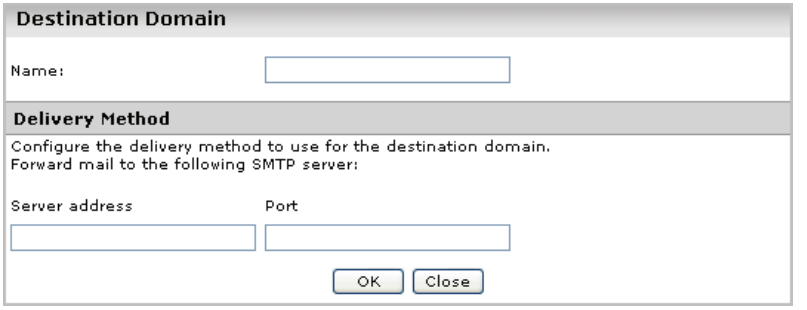
- domain1.com,192.168.1.1:2000
- domain2.net,192.168.2.2:1029
- domain3.com,smtp.domain3.com:25
- domain4.com,mail.domain4.com:2000

To specify the Domain-based Delivery:

1. Choose **Administration > IMSS Configuration > SMTP Routing** from the menu.
2. Click the **Domain-based Delivery** tab. The Domain-based Delivery screen appears.



3. Click **Add**, under Domain-Based Delivery. The Destination Domain screen appears.



4. Specify the **Destination Domain** and **Delivery Method**.
5. Click **OK**.
6. Click **Save**.

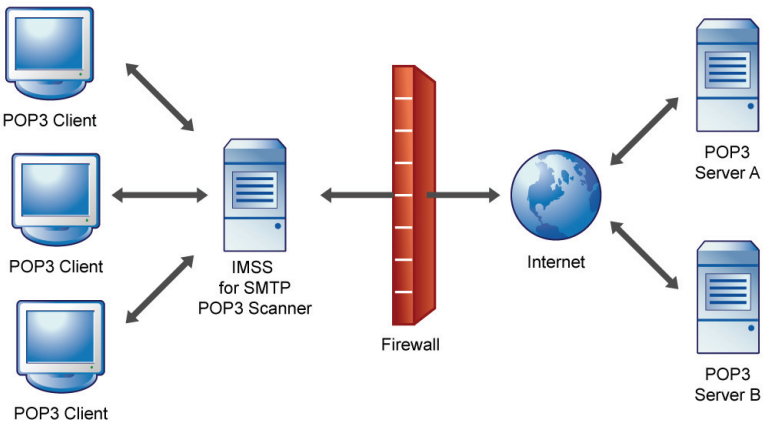
Scanning POP3 Messages

In addition to SMTP traffic, IMSS can scan POP3 messages at the gateway as clients in your network retrieve them. Even if your company does not use POP3 email, your employees might access their personal POP3 email accounts using mail clients on their computers. Hotmail® or Yahoo!® accounts are some examples of POP3 email accounts. This can create points of vulnerability on your network if the messages from those accounts are not scanned.

Understanding POP3 Scanning

The IMSS POP3 scanner acts as a proxy server (positioned between mail clients and POP3 servers) to scan messages as the clients retrieve them.

FIGURE 2-1. Scanning POP3 messages



To scan POP3 traffic, configure your email clients to connect to the IMSS server POP3 proxy, which connects to POP3 servers to retrieve and scan messages.

You can set up the following connection types:

- **Generic:** Allows you to access different POP3 servers using the same port, typically 110, the default port for POP3 traffic.

- **Dedicated:** Accesses the POP3 server using a specified port. Use these connections when the POP3 server requires authentication using a secure logon, such as APOP or NTLM.

Requirements

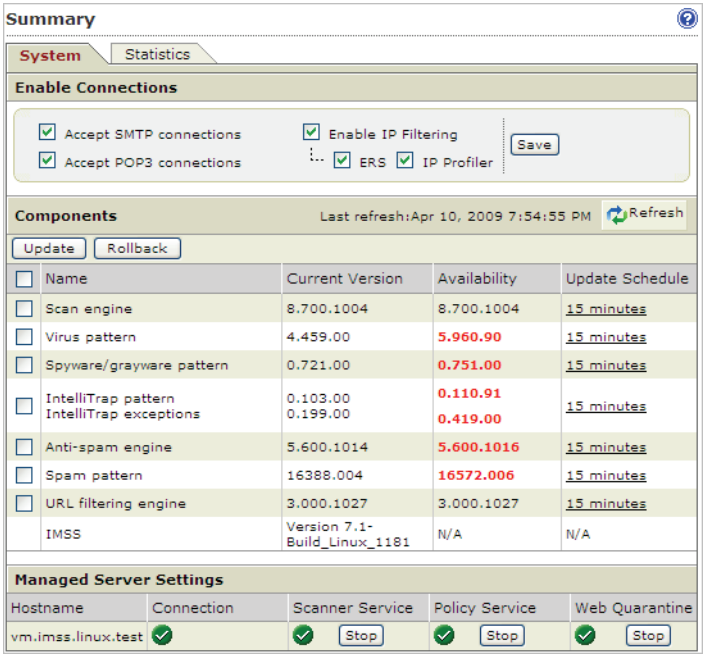
For IMSS to scan POP3 traffic, a firewall must be installed on the network and configured to block POP3 requests from all the computers on the network, except the IMSS server. This configuration ensures that all POP3 traffic passes to IMSS through the firewall and that IMSS scans the POP3 data flow.

Enabling POP3 Scanning

Before IMSS can begin scanning POP3 traffic, enable POP3 scanning and configure POP3 settings.

To enable POP3 scanning:

1. Choose **Summary** from the menu. The System tab appears by default.



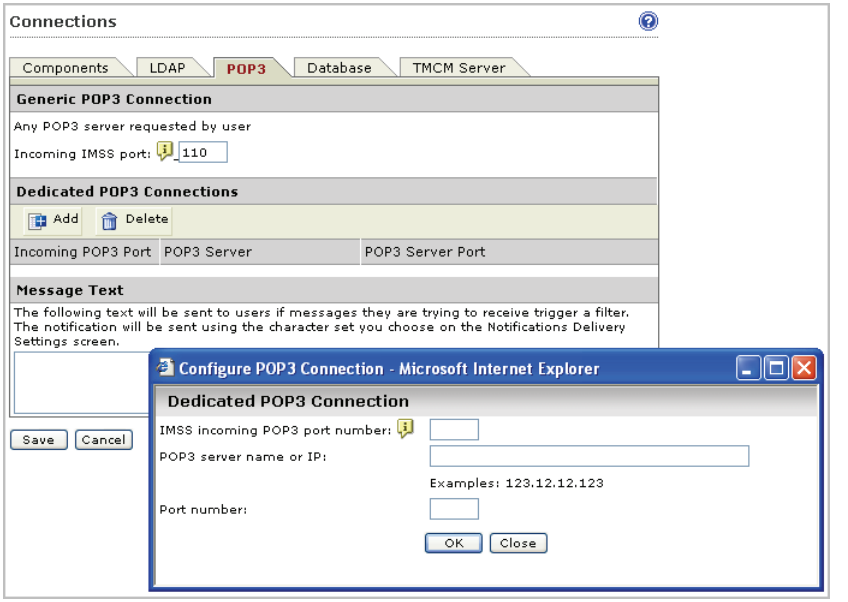
2. Select the check box next to **Accept POP3 connections**.
3. Click **Save**.

Configuring POP3 Settings

You can specify the IMSS server ports that clients will use to retrieve POP3 traffic. The default POP3 port is 110. However, if your users need to access a POP3 server through an authenticated connection, (through the APOP command or using NTLM) you may also set up a dedicated connection and assign a custom port.

To add a POP3 connection:

1. Choose **Administration** > **IMSS Configuration** > **Connections** from the menu. The Components tab appears by default.
2. Click the **POP3** tab.



3. Do one of the following:
   - To accept any POP3 server requested by user, type the incoming IMSS port number, if it is different from the default port 110.
   - To access the POP3 server using a specific port for authentication purposes, click **Add** to create a new dedicated POP3 connection. Provide the required information and click **OK**.
4. Click **Save**.

Chapter 3

Managing Policies

This chapter provides instructions for creating, modifying, and managing IMSS policies.

Topics include:

Managing Policies

IMSS policies are rules that are applied to incoming/outgoing email messages. Create rules to enforce your organization's antivirus and other security goals. By default, IMSS includes a Global Antivirus rule to help protect your network from viruses and related Internet threats. Because an antivirus rule addresses the most critical and potentially damaging types of messages, you should always keep it in the first position on the rule list so IMSS can analyze traffic for virus content first.

The antivirus rule does not protect against spam. For the best protection against spam, configure a custom rule that includes spam in the scanning conditions, and activate the IP Filtering product.

Note: Before creating a new policy, ensure that you have defined the internal addresses.

How the Policy Manager Works

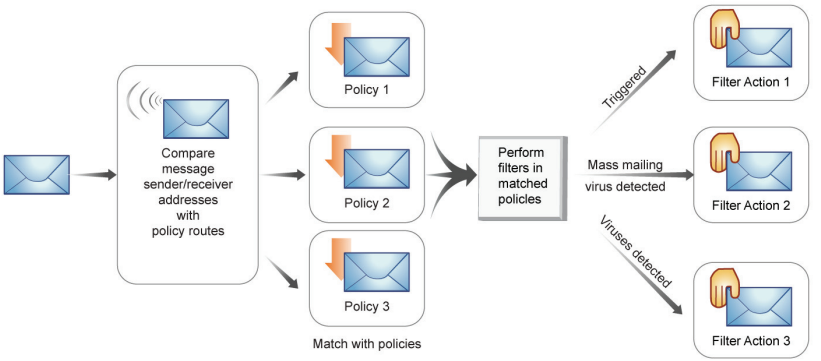
You can create multiple rules for the following types of policies. Use policies to reduce security and productivity threats to your messaging system:

- **Antivirus:** Scans messages for viruses and other malware such as spyware and worms.
- **Others:** Scans spam or phishing messages, message content, and other attachment criteria.

An IMSS policy has the following components:

- The **Route:** A set of sender and recipient email addresses or groups to which the policy is applied. You can use the asterisk (*) to create wildcard expressions and simplify route configuration.
- The **Filter:** A rule or set of rules that apply to a specific route, also known as scanning conditions. IMSS contains predefined filters that you can use to combat common virus and other threats. You can modify these predefined filters or define your own filters.
- The **Action:** The action that IMSS performs if the filter conditions are met. Depending on the filter result, a filter action is performed that determines how the message is finally processed.

FIGURE 3-1. Simplified policy manager process flow



For more information on how to create a policy, see *Adding Policies* on page 3-29.

To filter policies that display in the policy list:

1. Click **Policy > Policy List**. The Policy screen appears.
2. Configure the Filter by options:
   a. Specify a route:
      - **All routes:** Displays all policies
      - **Incoming:** Displays policies that only monitor incoming messages
      - **Outgoing:** Displays policies that only monitor outgoing messages
      - **Both directions:** Displays policies that monitor "incoming", "outgoing", and "incoming and outgoing" messages
      - **POP3:** Displays policies that only monitor POP3 messages
   b. Specify the type of protection the policy provides:
      - **All types**
      - **Viruses and malware**

- **Spyware and spam**
- **Web Reputation**
- **Attachments**
- **Content**
- **Size**
- **Other**

c. Specify the users the policy protects:

- **All Groups**
- **[Find user or group]**

Configuring Common Policy Objects

Common policy objects are items that can be shared across all policies, making policy creation easier for administrators.

TABLE 3-1. Common Policy Objects

COMMON POLICY OBJECTS	DESCRIPTION
Address Groups	Organize multiple email addresses into a single group.
Keywords & Expressions	Create keywords or expressions to prevent information leaks, block spam, or block derogatory email from entering or moving in your network.
Notifications	Create messages to notify a recipient or email administrator that IMSS took action on a message's attachment or that the message violated IMSS rule scanning conditions.
Stamps	Create stamps to notify a recipient that IMSS took action on a message's attachment or that the message violated scanning conditions for rules.

TABLE 3-1. Common Policy Objects

COMMON POLICY OBJECTS	DESCRIPTION
DKIM Approved List	Messages from domains with matched DKIM signatures will not be scanned or marked as spam.
Web Rep. Approved List	Domains appearing in the Web Reputation Approved List will not be scanned or blocked by Web reputation filters. However, other filters could block messages on the Web Reputation Approved List.

Understanding Address Groups

An address group is a list of email addresses to which your policy applies. Address groups allow you to organize multiple email addresses into a single group and apply the same policy to every address in the group.

For example, you have identified three types of content that you do not want transmitted through your company's email system and have defined three filters (in parentheses) to detect these types of content:

- Sensitive company financial data (FINANCIAL)
- Job search messages (JOBSEARCH)
- VBS script viruses (VBSCRIPT)

Consider the following address groups within your company:

- All Executives
- All HR Department
- All IT Development Staff

The filters that you use in the policies will be applied to these groups as follows:

ADDRESS GROUPS	FINANCIAL	JOBSEARCH	VBSCRIPT
All Executives	Not applied	Applied	Applied
All HR Department	Applied	Not applied	Applied
All IT Development Staff	Applied	Applied	Not applied

Executives, HR staff, and IT developers have legitimate business reasons to send financial information, job search-related correspondence and VBS files, respectively, so you would not apply some filters to those groups.

In IMSS, email addresses identify the different members of your organization and determine the policies that are applied to them. Defining accurate and complete address groups ensures that the appropriate policies are applied to the individuals in those groups.

Creating Address Groups

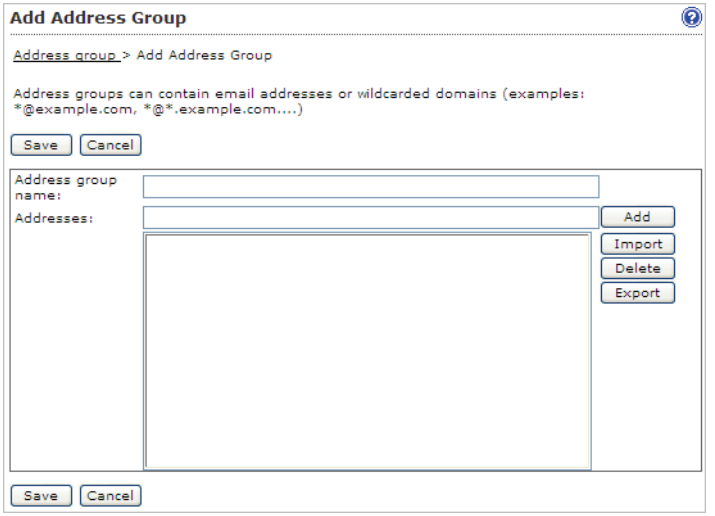
An address group is a collection of user email addresses in your organization. If you create an address group, you can apply rules to several email addresses at the same time, rather than applying rules to each address individually.

You can create address groups before creating any policies or when specifying the route during policy creation. You can also add an address group when modifying an existing policy. Create address groups manually or import them from a text file that contains one email address per line.

Tip: While address groups can be created during policy creation, Trend Micro recommends creating address groups before you begin creating policies.

To create an address group:

1. Choose **Policy** > **Address Groups** from the menu. The Address Groups screen appears.
2. Click **Add**. The Add Address Group screen appears.



3. Type a group name, then do any of the following:

Add an individual address:

- Type an email address and click **Add** to add email addresses individually. You can also use wildcard characters to specify the email address. For example, *@hr.com.

Import an address list:

a. Click **Import**. The Import Address group screen appears.

b. Type the file path and file name to import or click **Browse** and locate the file.

c. Select one of the following:

- **Merge with current list**
- **Overwrite current list**

d. Click **Import**.

Note: IMSS can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

---

4. Click **Save**. The Address Groups screen appears with the new address group appearing in the Address Groups table.

Adding an Address Group During Policy Creation

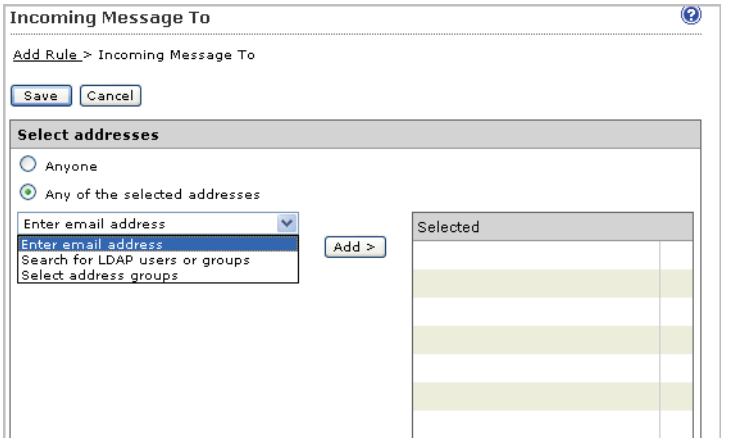
You can create an address group when specifying the route during policy creation. This can be done by adding email addresses individually or importing them from a text file.

Note: IMSS can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

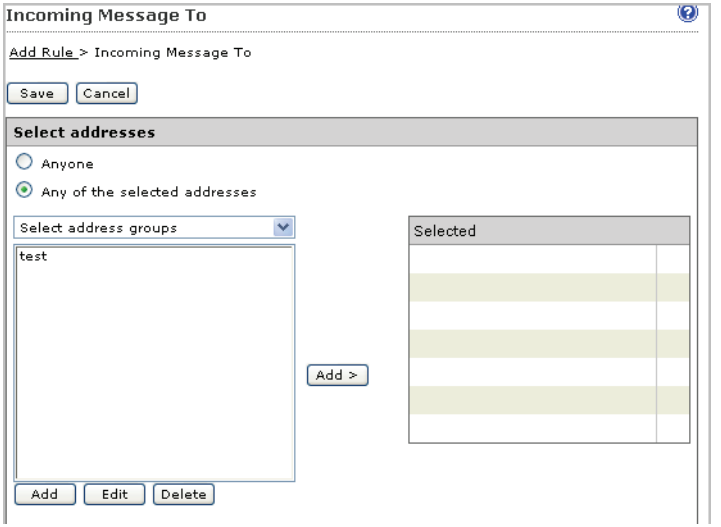
To add an address group:

1. Choose **Policy** > **Policy List** from the menu.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats. The Step 1: Select Recipients and Senders screen appears.

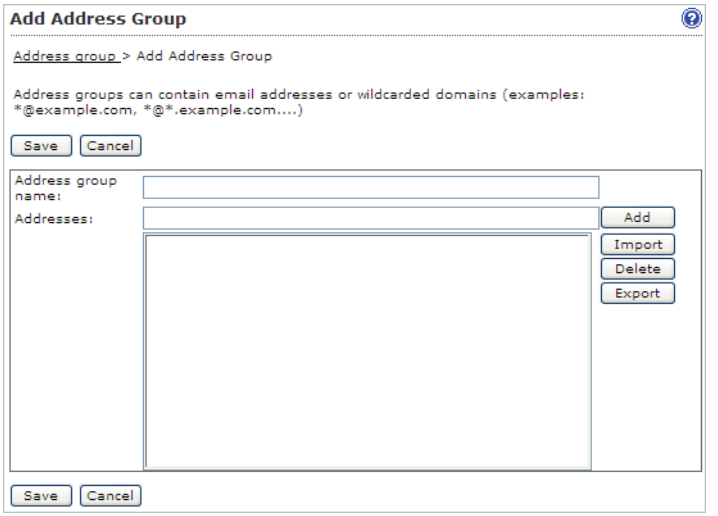
4. Click the **Recipients** or **Senders** link. The Select Addresses screen appears.



5. Choose **Select Address Groups** from the drop-down list.



6. Click the **Add** button. The Add Address Group screen appears.



7. Type a group name, then do one of the following:

Add an individual address:

- Type an email address and click **Add** to add email addresses individually. You can also use wildcard characters to specify the email address. For example, *@hr.com.

Import an address list:

a. Click **Import**. The Import Address group screen appears.

b. Type the file path and file name to import or click **Browse** and locate the file.

c. Select one of the following:

- **Merge with current list**
- **Overwrite current list**

d. Click **Import**.

Note: IMSS can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

---

8. Click **Save**.

Editing or Deleting an Address Group

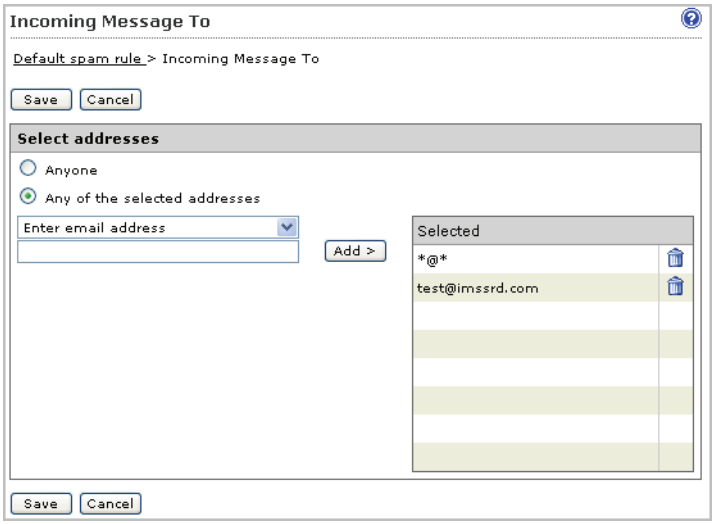
You can edit or delete an address group from the Address Groups screen or by editing an existing policy.

To edit or delete an address group:

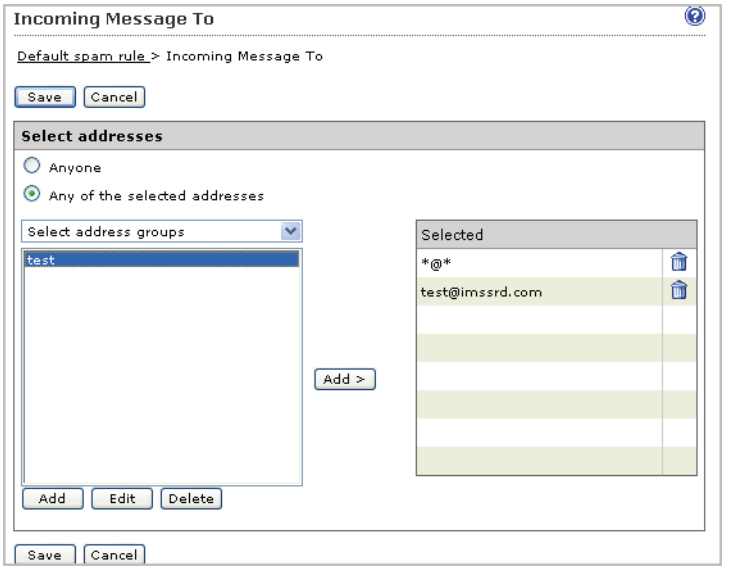
1. Click **Policy** > **Address Groups** from the menu. The Address groups screen appears.
2. To edit an address group:
   a. Click an existing address group from the Address Group table. The Add/Edit Address Group screen appears.
   b. Edit the address group as required.
   c. Click **Save**. The Address Groups screen appears.
3. To delete an address group:
   a. Select the check box next to an address group.
   b. Click **Delete**.

To edit or delete an address group from an existing policy:

1. Choose **Policy** > **Policy List** from the menu.
2. Click the link for an existing policy.
3. Click the **If recipients and senders are** link.
4. Click the **Recipients** or **Senders** link. The Select addresses screen appears.



5. Choose **Select address groups** from the drop-down list.



6. Select the desired address group and click the **Edit** or **Delete** button accordingly.

Exporting an Address Group

Export address groups to import to other IMSS servers. Export from existing policies or from the Address Group list.

To export an address group:

1. Choose **Policy** > **Address Groups** from the menu. The Address Groups screen appears.
2. Click the address group to export. The Address Group screen appears.
3. Click **Export**. The File Download screen appears.
4. Click **Save**. The Save As dialog box appears.
5. Specify the name and location to export the address group.
6. Click **Save**.

To export an address group from an existing policy:

1. Choose **Policy** > **Policy List** from the menu.
2. Click the link for an existing policy.
3. Click the **If recipients and senders are** link.
4. Click the **Recipients** or **Senders** link. The Select addresses screen appears.
5. Choose **Select address groups** from the drop-down list. The Address Group screen appears.
6. Click **Export**. The File Download screen appears.
7. Click **Save**. The Save As dialog box appears.
8. Specify the name and location to export the address group.
9. Click **Save**.

Using the Keyword & Expression List

IMSS can take action on an email message based on the content in the subject line, body, or header. To filter by message content, add and enable keywords or regular expressions to a keyword expression list. You can configure several expression lists and enable or disable them at any time. To configure a list that is very similar to an existing list, copy a list and then edit the copy.

To select scanning conditions for content:

1. Create or modify an "Other" (not an Antivirus) policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. Under **Content**, on the Scanning Conditions screen, select the check boxes next to the parts of an email message to which you want the content conditions to apply.
3. Click the link that specifies the part of the email message to which you want to configure content conditions. The Keyword Expressions screen appears with two columns:
   - **Available:** Expressions available for use, but not currently in use.
   - **Selected:** Expressions currently in use.

4. If you are configuring expressions for the header, select the check boxes next to the header items where the expression will apply.
5. Click **Add**. The screen for managing keyword expressions appears.
6. Configure the expressions.
7. In the **Available** list, click the expression list you want to enable.
8. Click **>>**. The expressions appear in the Selected list.

   To keep an expression list available but temporarily prevent IMSS from using it, click the expression in the selected list, and then click **<<**.
9. Click **Save** to continue to the scanning conditions selection screen.

Configuring an Expression

Configure keyword and regular expressions to enable IMSS to scan email message content. You can create keywords or expressions from the Keywords & Expressions screen or during rule creation.

Tip: While keywords or expressions can be created during policy creation, Trend Micro recommends creating keywords or expressions before you begin creating policies.

To create keywords or expressions:

1. Click **Policy > Keywords & Expressions**. The Keywords & Expressions screen appears.
2. Click **Add**. The **Add/Edit Keyword & Expression** screen appears.
3. Next to **List name**, type a descriptive name.
4. Next to **Match**, select one of the following that specifies when IMSS takes action:
   - **Any specified:** Email message content can match any of the expressions in the list.
   - **All specified:** Email message content must match all the expressions in the list.
   - **Not the specified:** Email message content must not match any of the expressions in the list.
   - **Only when combined score exceeds threshold:** Next to **Total message score to trigger action**, type a number that represents the maximum score for allowed keyword expressions. When you add an expression, you can set a score for it.

5. To create an expression, click **Add**. The Add Keyword Expression list appears.
6. Type the keywords. For a partial match, type the keyword. To specify an exact match, use "\s" (without the quotes) before and after the keyword.

   For example:

   - keyword matches "keywords", "akeyword", etc.
   - \skeyword\s matches "keyword" only.
7. Click **Save**. The Add Keyword Expression list appears.
8. To instruct IMSS to consider the capitalization of email content when it uses the filter, select the check box under **Case sensitive**.
9. If you selected **Only when combined score exceeds threshold**, select a score from the drop down box.
10. Click **Save**. The Keywords & Expressions screen appears with the new keyword or expression appearing in the table.

To add or edit a keyword or expression during policy creation or modification:

1. Create or modify an "Other" (not an Antivirus) policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. Under **Content** on the Scanning Conditions screen, click the link that specifies the part of the email message to which you want to configure content conditions. The Keyword Expressions screen appears with two columns:
3. Click **Add** or **Edit** from the Keyword Expressions screen. The configuration screen for keyword expression lists appears.
4. Next to **List name**, type a descriptive name.
5. Next to **Match**, select one of the following that specifies when IMSS takes action:
   - **Any specified:** Email message content can match any of the expressions in the list.
   - **All specified:** Email message content must match all the expressions in the list.
   - **Not the specified:** Email message content must not match any of the expressions in the list.

- **Only when combined score exceeds threshold:** Next to **Total message score to trigger action**, type a number that represents the maximum score for allowed keyword expressions. When you add an expression, you can set a score for it.

6. To create an expression, click **Add**. The Add Keyword Expression list appears.
7. Type the keywords. For a partial match, just type the keyword. To specify an exact match, use "\s" (without the quotes) before and after the keyword.

   For example:

   - keyword matches "keywords", "akeyword", etc.
   - \skeyword\s matches "keyword" only.
8. If you selected **Only when combined score exceeds threshold**, select a score from the drop down box.
9. Click **Save**. The configuration screen for keyword expression lists reappears with the expression in the list.
10. To instruct IMSS to consider the capitalization of email content when it uses the filter, select the check box under **Case sensitive**.
11. Click **Save** to continue modifying or creating the policy.

Using the Notifications List

To notify a recipient or an email administrator that IMSS performed action on a message's attachment or that the message violated IMSS rule scanning conditions, send a notification.

For details about adding to the policy notifications list see, Adding or Modifying a Policy Notification on page 3-18.

To send policy notifications:

1. Create or modify a policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. Under **Monitor**, on the Select Actions screen during policy modification or creation, click **Send policy notifications**. The Notifications screen appears with two columns:

- **Available:** Notification messages available for use, but not currently in use.
- **Selected:** Notification messages currently in use.

3. Add or modify a notification.
4. In the **Available** list, click the notifications you want to enable.
5. Click >>. The notifications appear in the **Selected** list.

   To keep a notification available but temporarily prevent IMSS from using it, click the notification in the selected list, and then click **<<**.
6. Click **Save** to continue creating or modifying the policy.

Adding or Modifying a Policy Notification

Create policy notifications from the Policy Notifications screen or during policy creation or modification.

Tip: While keywords or expressions can be created during policy creation, Trend Micro recommends creating keywords or expressions before you begin creating policies.

To add or modify a policy notification:

1. Click **Policy > Policy Notifications**. The Policy Notifications screen appears.
2. Click **Add**. The Add/Edit Policy Notification screen appears.
3. Configure the following:
   - **Name:** Type a descriptive name for the notification.
   - **From:** Type a sender email address.
   - **To:** Type the receiver email addresses and select the check boxes next to **Original Mail Sender** and/or **Original Mail Recipient**. Separate each address with a semicolon (;).
   - **Subject:** Type the subject line of the notification.
   - **Message:** Type the notification message.
4. To send the original message as an attachment of the notification message, select the check box next to **Attach the message**.
5. To see the types of variables you can include in the message, click **Variables list**.
6. To send an SNMP trap, configure the following:
   a. Click one of the following:

- **Disable (first radio button):** Avoid sending any trap IDs.
- **Second radio button:** Select one of the default SNMP traps.
- **Third radio button:** Type a custom trap ID.

b. **Message:** Type the notification message.

7. Click **Save**.

To add or modify a policy notification during policy creation or modification:

1. Create or modify a policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. Under **Monitor**, on the Select Actions screen, click **Send policy notifications**. The Notifications screen appears with two columns:
   - **Available:** Notification messages available for use, but not currently in use.
   - **Selected:** Notification messages currently in use.
3. Click **Add** or **Edit**. The configuration screen for the notification appears.
4. To send an email notification, configure the following:
   - **Name:** Type a descriptive name for the notification.
   - **From:** Type a sender email address.
   - **To:** Type the receiver email addresses and select the check boxes next to **Original Mail Sender** and/or **Original Mail Recipient**. Separate each address with a semicolon (;).
   - **Subject:** Type the subject line of the notification.
   - **Message:** Type the notification message.
5. To send the original message as an attachment of the notification message, select the check box next to **Attach the message**.
6. To see the types of variables you can include in the message, click **Variables list**.
7. To send an SNMP trap, configure the following:

   a. Click one of the following:
   - **Disable (first radio button):** Avoid sending any trap IDs.
   - **Second radio button:** Select one of the default SNMP traps.
   - **Third radio button:** Type a custom trap ID.

b. **Message:** Type the notification message.

8. Click **Save**.

Using Stamps

To notify a recipient that IMSS took action on a message's attachment or that the message violated scanning conditions for rules, add a stamp to the beginning or end of the email message body.

Tip: Add stamps only for email that the intended recipients will eventually receive. If you are configuring a rule to delete messages that violate your scanning conditions, adding a stamp is not necessary.

To use stamps in a policy:

1. Create or modify a policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. While creating or modifying a policy on the Select Actions screen, select the check box next to **Insert stamp in body** or **Insert safe stamp for clean mails** under Modify.

Creating Stamps

Create stamps from the Stamps screen or during policy creation or modification.

Tip: While stamps can be created during policy creation, Trend Micro recommends creating stamps before you begin creating policies.

To create a stamp:

1. Click **Policy > Stamps**. The Stamps screen appears.
2. Click **Add** or select a stamp to edit from the Stamp list.. The Add/Edit Stamp screen appears.
3. Next to **Name**, type the name of the stamp

4. Next to **Insert at**, click **End of message body** or **Beginning of message body**.
5. Under **Text**, type the message. To see the types of variables you can include in the message, click **Variables list**.
6. To prevent possible damage to TNEF-encoded messages or digitally signed messages, select **Do not stamp TNEF-encoded messages or digitally signed messages**.
7. Click **Save** to return to the Stamps screen.

To create a stamp during policy creation or modification:

1. Create or modify a policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. Under **Modify**, on the Select Actions screen, click **Edit** next to **Insert stamp in body** or **Insert safe stamp for clean mails**. The Stamps screen appears showing the available stamps.
3. To add a new stamp, click **Add**. To modify an existing stamp, click it in the list box and then click **Edit**. An edit screen appears.
4. Next to **Name**, type the name of the stamp
5. Next to **Insert at**, click **End of message body** or **Beginning of message body**.
6. Under **Text**, type the message. To see the types of variables you can include in the message, click **Variables list**.
7. To prevent possible damage to TNEF-encoded messages or digitally signed messages, select **Do not stamp TNEF-encoded messages or digitally signed messages**.
8. Click **Save** to return to the Stamps screen.
9. Click **Done**.

Using the DKIM Approved List

DomainKeys Identified Mail (DKIM) is a signature/cryptography-based email authentication that provides a method for validating an email during its transfer over the Internet. By validating that the email comes from the source it is claiming, IMSS provides spam and phishing protection for your network. Validated email messages are

not marked as spam and are not scanned for spam. This means false positives are reduced as is the need for scanning email messages from a source that is known to be safe.

To enable the DKIM Approved List:

1. Click **Policy > DKIM Approved List**. The DKIM Approved List screen appears.
2. Select the **Enable the DKIM Approved List for use in policies** check box.
3. Populate the list with known safe domains.

   Manually:

   a. Type a domain name.

   b. Click **Add**.

   Import a list:

   Note: When importing a text file for the DKIM Approved List, only one domain should be on each line.

   a. Click **Import**. The Import DKIM Approved List appears.

   b. Type the file path and file name or click **Browse** and locate the file.

   c. Select one of the following:

      - **Merge with current list**
      - **Overwrite current list**

   d. Click **Import**.
4. Click **Save**.

Using the Web Reputation Approved List

Web reputation can protect users on your network from malicious URLs in email messages. Web reputation does this by scanning URLs in email messages and then comparing the URL with known malicious URLs in the Trend Micro Web reputation database. The Web Reputation Approved List provides administrators with a way to bypass scanning and blocking of URLs which the administrator knows to be safe.

To enable the Web Reputation Approved List:

1. Create or modify an "Other" (not an Antivirus) policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. Under **Web Reputation** on the Scanning Conditions screen, click Web Reputation settings. The Web Reputation Settings screen appears.
3. Select the **Enable the use of the Web Reputation Approved List** check box.
4. Click **Save**. The Step 2: Select Scanning Conditions screen appears.
5. Continue configuring the policy.

Adding to the Web Reputation Approved List

Domains added to the Web Reputation Approved List will not be scanned by IMSS. Administrators should only add domains they know to be safe.

To add domains to the Web Reputation Approved List:

1. Click **Policy > Web Rep. Approved List**. The Web Reputation Approved List screen appears.
2. Populate the Web Reputation Approved List in one of the following ways:

   Manually:

   a. Type a domain. For example: `*.trendmicro.com`.

   b. Click **Add**>>.

   Import a list:

   Note: When importing a text file for the Web Reputation Approved List, only one domain should be on each line.

   a. Click **Import**. The Import Web Reputation Approved List appears.

   b. Type the file path and file name or click **Browse** and locate the file.

   c. Select one of the following:

      - **Merge with current list**

- **Overwrite current list**

d. Click **Import**.

3. Click **Save**.

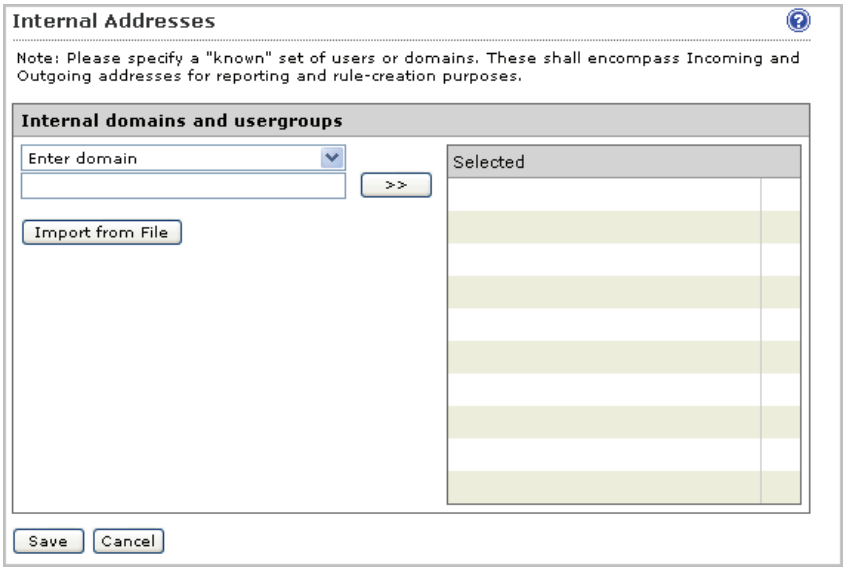
Configuring Internal Addresses

For reporting and rule creation, IMSS uses internal addresses to determine which policies and events are Inbound and Outbound:

- For incoming messages, specify the recipient's address, which is in range of the internal addresses. (for example: internal address is imsstest.com, valid recipients include jim@imsstest.com, bob@imsstest.com)
- For outgoing messages, specify the sender's address, which is in range of the internal addresses. (for example: internal address is imsstest.com, valid senders include jim@imsstest.com, bob@imsstest.com)
- For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

To set internal addresses:

1. Choose **Policy > Internal Addresses** from the menu. The Internal Addresses screen appears.



2. Under **Internal Domains and User Groups**, choose one of the following from the drop-down box:
   - **Enter domain**: Type a domain and click >>. Do not type the "@" or user name parts of an email address. For example, domainname or domainname1.domainname2 are valid; user@domainname is invalid.

Note: You can use wildcards for domain names. For example, use *.domain.com to include all sub-domains for "domain.com". However, you cannot use two asterisks in the user name or domain name portion of the address or use the "@" symbol. *.*@domain.com and user@*.* are both invalid.

- **Search for LDAP group:** A screen for searching the LDAP groups appears. Type an LDAP group name (not an individual LDAP user) for which you want to search in the text box and click **Search**. The search result appears in the list box. To add it to the Selected list, click the LDAP group and then click >>.

  For more information, see Searching for an LDAP User or Group on page 3-27.

Note: When selecting an LDAP group for the internal addresses, you can use wildcards in the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server. For example, A*, *A, and *A* are all allowed.

If you have selected Domino as the LDAP server, you can only use wildcards at the end. For example, *A and *A* are not allowed.

---

3. To import domains from a file, click **Import from File** and select the file.

Tip: Import both the exact domain and all sub-domains for best results.

The following shows sample content of a domain list text file:

- domain.com: Imports the exact domain
- *.domain.com: Imports all sub-domains
- domain.org: Imports the exact domain

Note: The import file must be a text file containing one domain per line. You can use wildcards when specifying the domain.

---

4. Click **Save**.

To export internal addresses:

1. Choose **Policy > Internal Addresses** from the menu. The Internal Addresses screen appears.
2. Click **Export**. A File Download dialog box appears.
3. Click **Save**. A Save As dialog box appears.

4. Specify the location and file name.
5. Click **Save**.

Searching for an LDAP User or Group

When specifying the route for a policy, instead of entering an individual email address or address group, you can also perform a search for a Lightweight Directory Access Protocol (LDAP) user or group.

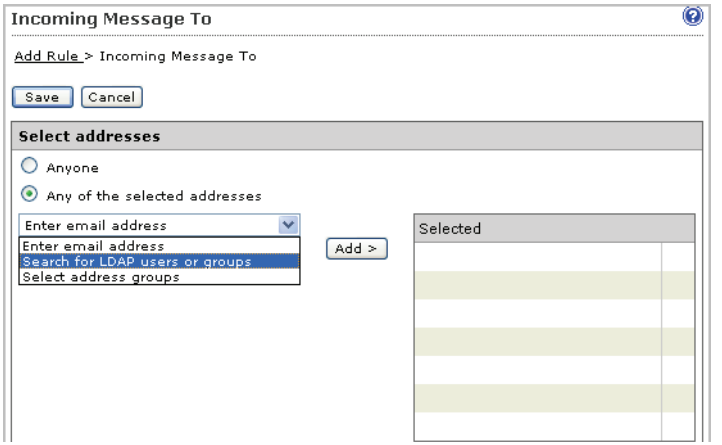
IMSS supports the following three (3) types of LDAP servers:

- Microsoft™ Active Directory 2000 or 2003
- IBM™ Lotus™ Domino™ 6.0 or above
- SUN Microsystems™ One LDAP

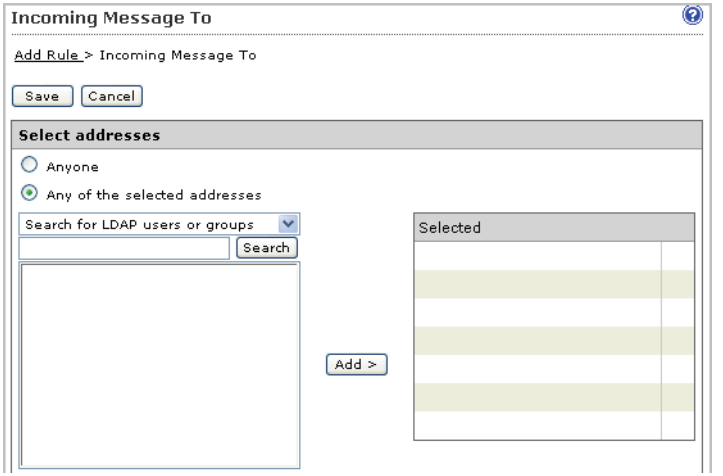
The following steps provide instructions on adding an LDAP user or group when creating a new policy.

To add an LDAP user or group:

1. Choose **Policy** > **Policy List** from the menu.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats respectively.
4. Click the **Recipients** or **Senders** link. The Select Addresses screen appears.



5. Choose **Search for LDAP users or groups** from the drop-down list.



6. Type the LDAP user or group that you want to search.

Note: 1. You can use the asterisk wildcard when performing a search. See Using the Asterisk Wildcard on page 3-70.

2. You can also search for LDAP groups when adding internal addresses. For more information, see Configuring Internal Addresses on page 3-24.

7. Click the **Search** button.
8. IMSS displays the LDAP user or group if a matching record exists on the LDAP server.
9. Select the user or group and click the **Add** button to add it to the recipient or sender list.

Adding Policies

Before creating a policy, ensure that you have configured the internal addresses. For more information, see Configuring Internal Addresses on page 3-24.

Creating a policy involves the following steps:

Step 1. Specifying a Route on page 3-29

Step 2. Specifying Scanning Conditions on page 3-36

Step 3. Specifying Actions on page 3-51

Step 4. Finalizing a Policy on page 3-59

Tip: To prevent a virus leak and ensure that all messages are scanned, Trend Micro recommends that you maintain at least one antivirus rule that applies to **all messages**. Select **all messages** from the drop-down list when specifying the route for an antivirus rule.

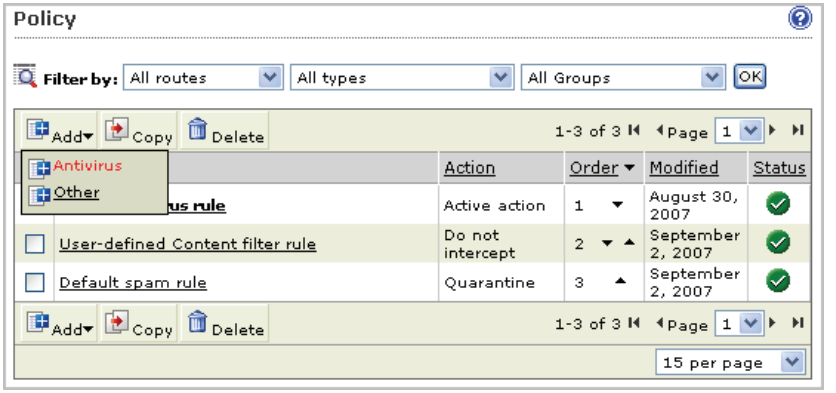
Specifying a Route

The first step in adding a rule is configuring the following:

- **The route:** A specific "To" and "From" combination that includes a recipient's and sender's email address, LDAP users or groups, or address groups. You can also configure exceptions to a route.
- **Route type:** The direction of SMTP traffic, POP3 traffic, or all traffic.

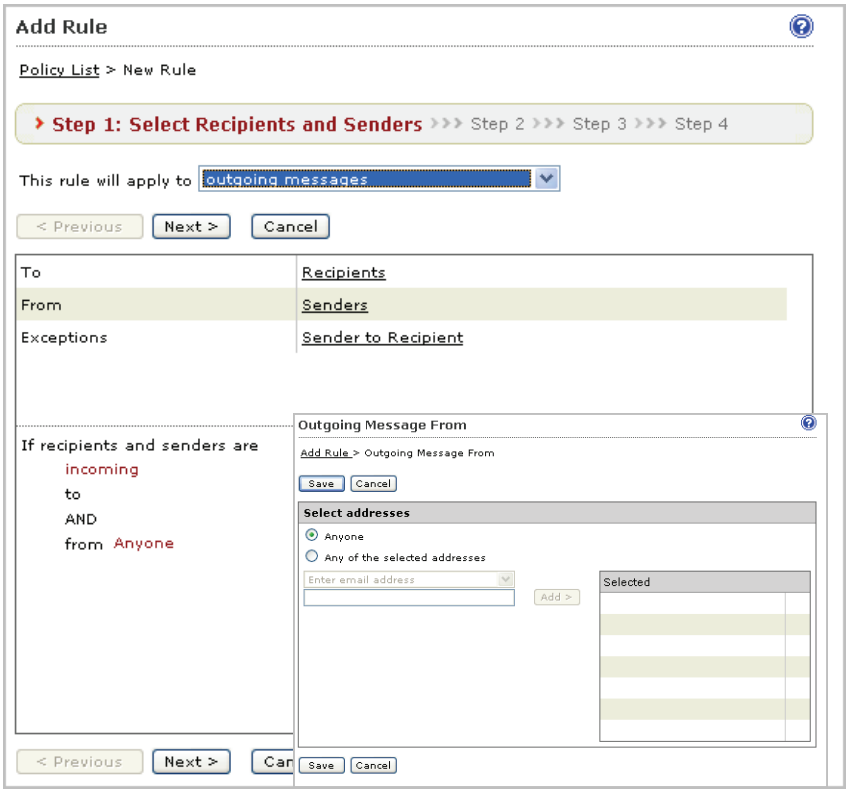
To add a route:

1. Choose **Policy > Policy List** from the menu. The Policy List screen appears.
2. Click **Add**.
3. Select **Antivirus** or **Other** from the drop-down list. The Add Rule screen appears.



Note: The **Antivirus** rule scans messages for viruses and other malware such as spyware and worms.

The **Other** rule scans spam or phishing messages, message content, and other attachment criteria.



4. Select the policy route type from the drop-down list next to **This rule will apply to**.
   - **incoming messages**
   - **outgoing messages**
   - **both incoming and outgoing messages**
   - **POP3**
   - **all messages**
5. Select the recipients and senders:

- For incoming messages, specify the recipient's address, which is in range of the internal addresses. (for example: internal address is imsstest.com, valid recipients include jim@imsstest.com, bob@imsstest.com)
- For outgoing messages, specify the sender's address, which is in range of the internal addresses. (for example: internal address is imsstest.com, valid senders include jim@imsstest.com, bob@imsstest.com)
- For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

Note: 1. You can use the asterisk wildcard when specifying an email address. For more information, see Using the Asterisk Wildcard on page 3-70.

2. If you selected POP3, you cannot configure the route. The rule applies to all POP3 routes.

3. If you selected "all messages" for a rule, the rule also applies to messages from any sender to any recipient.

---

6. Click **Next**. The Step 2: Select Scanning Conditions screen appears.

To edit a route for an existing policy:

1. Choose **Policy > Policy List** from the menu. The Policy List screen appears.
2. Click the name of the policy to edit. The Summary screen for the policy appears.
3. Click **Edit** for **If recipients and senders are**. The Recipients and Senders screen for the policy appears.
4. Select the policy route type from the drop-down list next to **This rule will apply to**.
   - **incoming messages**
   - **outgoing messages**
   - **both incoming and outgoing messages**
   - **POP3**
   - **all messages**

Note: The **This rule will apply to** option cannot be modified in the Global DKIM Enforcement rule.

5. Select the recipients and senders:
   - For incoming messages, specify the recipient's address, which is in range of the internal addresses. (for example: internal address is imsstest.com, valid recipients include jim@imsstest.com, bob@imsstest.com)
   - For outgoing messages, specify the sender's address, which is in range of the internal addresses. (for example: internal address is imsstest.com, valid senders include jim@imsstest.com, bob@imsstest.com)
   - For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

Note: 1. You can use the asterisk wildcard when specifying an email address. For more information, see Using the Asterisk Wildcard on page 3-70.

2. If you selected POP3, you cannot configure the route. The rule applies to all POP3 routes.

3. If you selected "all messages" for a rule, the rule also applies to messages from any sender to any recipient.

6. Click **Save**.

Configuring the Route

A route is a specific "To" and "From" combination that includes a recipients and senders email address, LDAP users or groups, or address groups. You can also configure exceptions to a route.

Senders and recipients must be on the Internal Addresses list if you select incoming messages or outgoing messages when adding a new rule or modifying an existing rule:

- If you are configuring an outgoing message, the Internal Address list applies to the senders.

- If you are configuring an incoming message, the Internal Address list applies to the recipients.

Examples

Use the asterisk wildcard to include a range of email addresses. For example:

- **user@company.com:** Adds only the specific address.
- ***@company.com:** Adds any user at the domain "company.com".
- ***@*.company.com:** Adds any user at any subdomain of "company.com". For example, "user1@accounting.company.com" would be included.
- ***@*:** Adds all addresses.

To configure the route:

1. Click one of the following on the Select Recipients and Senders screen:
   - **Recipients** or **Senders:** Appears if you selected incoming messages or outgoing messages.
   - **Users:** Appears if you selected both incoming and outgoing messages.
2. Under **Select addresses**, select one of the following:
   - **Anyone:** Select this option to remove any restriction on the recipients or senders.
   - **Enter address:** Type the email address to add.
   - **Search for LDAP users or groups:** Type the LDAP user or group name and click **Search**. The results display in the list box.
   - **Select address groups:** All existing address groups appear in the list. If there are a large number of email addresses that you will reuse for routes in several rules, click **Add** to create an address group.
3. If you are adding an email address or email address group, click **Add>**. If you are adding an LDAP or address group, click it in the list box, and then click **Add>**.
4. To remove any email address or email address group from the Selected list, click the trash can icon.
5. Click **Save**.

Tip: When selecting an LDAP group as the recipients or senders, you can use wildcards in the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server. For example, A*, *A, *A* are all allowed. If you have selected Domino as the LDAP server, you can only use wildcards at the end. For example, *A and *A* are not allowed.

To prevent virus leaks and ensure that all messages are scanned, Trend Micro recommends that you maintain at least one antivirus rule that applies to all messages at all times.

Configuring Exceptions for Routes

Do the following to configure a route that applies to a large group of senders or recipients, with the exception of specific users, to whom the rule does not apply.

To configure exceptions for routes:

1. Click the link next to **Exceptions**, on the Add Rule screen. The Exceptions screen appears for the traffic direction (incoming, outgoing, both incoming and outgoing messages, or all messages).
2. Under **Select addresses**, select one of the following for both the **From** and **To** addresses:
   - **Enter email address:** Type the email address to add.
   - **Search for LDAP users or groups:** Type the LDAP user or group name and click **Search**. The results display in the list box.
   - **Select address groups:** All existing address groups appear in the list. If there are a large number of email addresses that you will reuse for routes in a rule, click **Add** to create an address group.
3. If you are adding an email address, click **Add>**. If you are adding an LDAP or address group, click it in the list box, and then click **Add>**.
4. To remove a sender-recipient pair from the list, click the trash can icon.
5. Click **Save**.

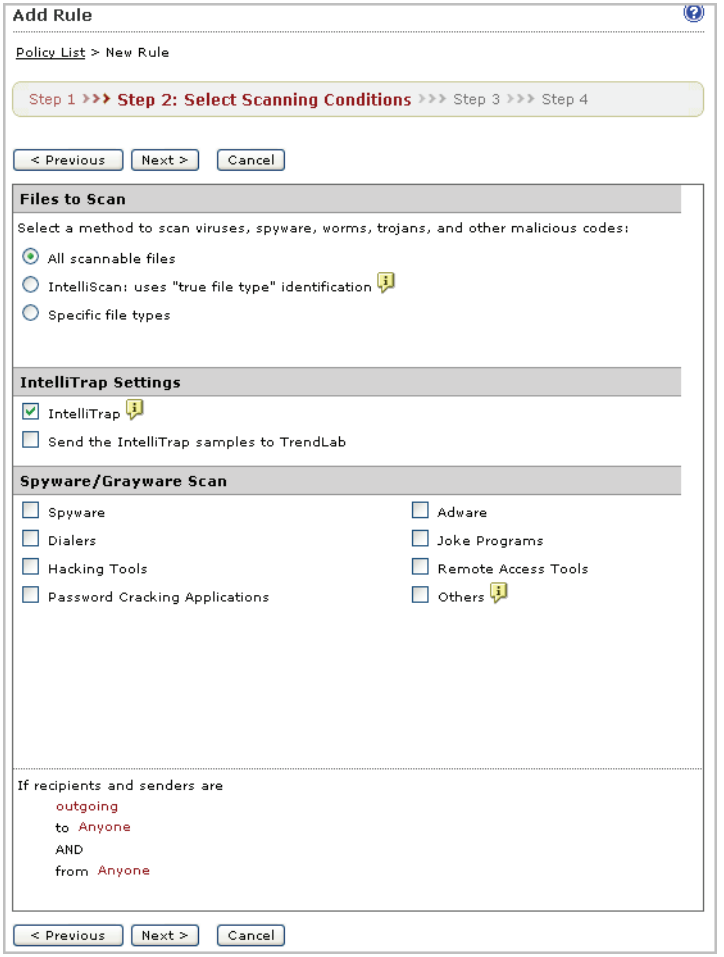
Specifying Scanning Conditions

After selecting the senders and recipients for a new rule or modifying the senders and recipients for an existing rule, configure the rules to filter email traffic based on several conditions.

The scanning conditions vary depending on whether Antivirus rules or Other rules are being created.

To specify scanning conditions:

1. Select the check boxes as desired, from the Step 2: Select Scanning Conditions screen. The categories of scanning conditions for the Antivirus and the Other rule types vary as follows:

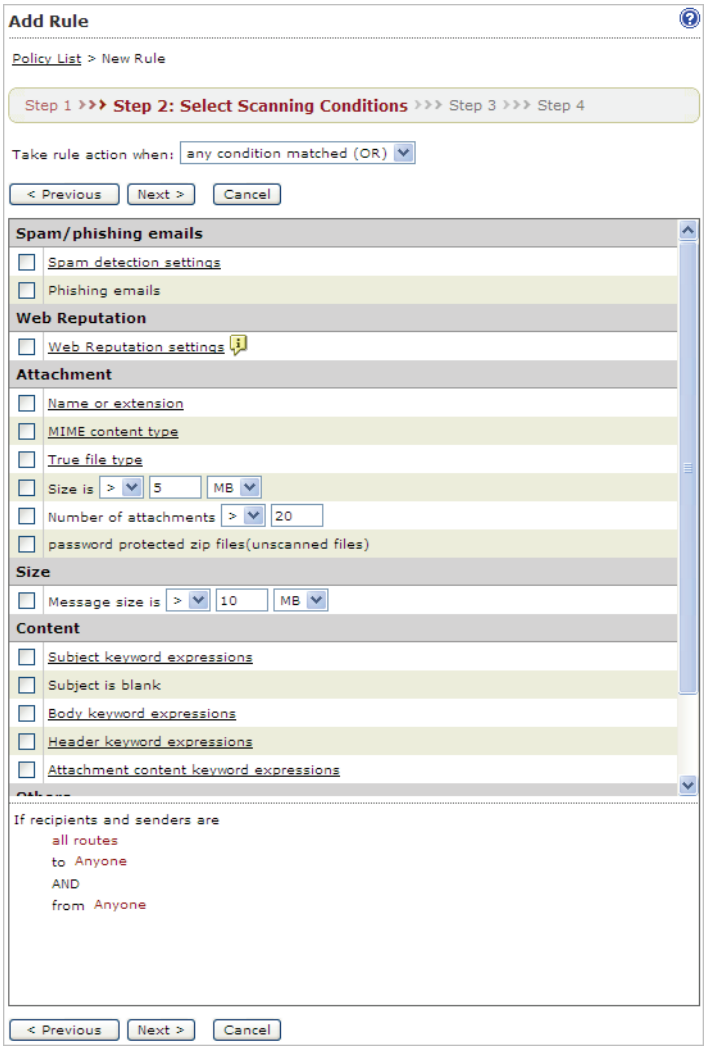


Antivirus rule

a. **Files to Scan:** Set the default method for scanning messages and specific file types containing viruses and other malware.
   - **All scannable files:** Attempt to scan all files.
   - **IntelliScan: uses "true file type" identification:** Use IntelliScan to identify malicious code that can be disguised by a harmless extension name.
   - **Specific file types:** Select the check box next to one of the following types of file extensions to scan:
     - **Application and executables:** Click the link and select the sub-types to scan.
     - **Documents:** Click the link and select the sub-types to scan.
     - **Compressed files:** Click the link and select the sub-types to scan.
     - **Specified file extensions:** Type the extension in the text box. You do not need to type the period (.) before the extension. You can also use an asterisk wildcard for the extension.

b. **IntelliTrap Settings:** Scan compressed files for viruses/malware and send samples to TrendLabs for investigation.
   - **IntelliTrap:** Scan email attachments that contain real-time compressed executable files.
   - **Send the IntelliTrap samples to TrendLabs:** IMSS can automatically send email messages with attachments that IntelliTrap catches to TrendLabs.

c. **Spyware/Grayware Scan:** Scan for other types of threats such as spyware and adware.



Other rule

a. Select one of the following next to **Take rule action when**, which specifies when IMSS can take action on an email message:

- **all conditions matched (AND):** When an email message matches all of the conditions.
- **any conditions matched (OR):** When an email message matches any of the conditions.

b. **Spam/phishing emails:** Scans messages identified as spam and phishing messages. Spam messages are generally unsolicited messages containing mainly advertising content. Phishing messages, on the other hand, originate from senders masquerading as trustworthy entities.

- **Spam detection settings:** Click the link to choose a level of spam protection and configure lists for approved and blocked senders and text exemptions.
- **Phishing emails**

c. **Web Reputation:** Scans URLs in messages to protect against phishing and other malicious Web sites.

d. **Attachment**: Scans messages for file attachments that match the selected criteria, such as attachments with specific extensions or belonging to a certain true file type.

- **Name or extension:** Click the link to configure filter settings for specific file names or extension names.
- **MIME content type:** Click the link to configure filter settings for MIME content types.
- **True file type:** Click the link to configure filter settings for common executable, document, image, media, and compressed files.
- **Size is {>, <, =} {size} {MB, KB, B}:** Choose to filter attachments of a size that is more than, less than, or equal to a certain number of bytes, kilobytes, or megabytes. Type a number that represents the file size.
- **Number is {>, <, =} {number}:** Choose to filter the number of attachments that is more than, less than, or equal to a certain number. Type a number that represents the total number of attachments for each email message.
- **Password protected zip files (unscanned files):** Choose to filter password protected files that cannot be scanned by IMSS.

e. **Size:** Scans messages that match the specified message size.

- **Message size is {>, <, =} {size} {MB, KB}:** Choose to filter email messages of a size that is more than, less than, or equal to a certain number of kilobytes, or megabytes. Type a number that represents the email message size.

f. **Content:** Scans messages containing the keyword expressions that match those expressions specified in the subject, body, header, or attachment content keyword expressions links.

- **Subject keyword expressions:** Click the link to manage your expression lists.
- **Subject is blank:** Select to filter email messages without a subject. Sometimes spam messages do not contain subject lines.
- **Body keyword expressions:** Click the link to manage your expression lists.
- **Header keyword expressions:** Click the link to manage your expression lists. Headers include Subject, To, From, CC, and other headers that you can specify.
- **Attachment content keyword expressions:** Click the link to manage your expression lists.

g. **Others**: Scans messages in which the number of recipients match the specified number. Also scans messages that are received within the specified time range.

- **Recipient number {>, <, =} {number}:** Choose to filter the number of recipients. Type a number that represents the total number of recipients for each email message.
- **Received time range:** Click the link to choose a day and time within which a message was received.
- **Encrypted messages:** Choose to filter encrypted messages that cannot be scanned by IMSS.

Selecting Scanning Conditions for Spam

Spam criteria includes a spam catch rate/detection threshold setting and configurable lists for approved and blocked senders and for text exemption rules.

To configure spam scanning conditions:

1. Under **Spam/phishing emails** on the scanning conditions selection screen for the Other rule type, select the check box next to **Spam detection settings**.
2. Click **Spam detection settings**. The Spam detection settings screen appears.
3. To enable spam scanning, select the check box next to Select a spam catch rate or specify a detection threshold. If you do not select this check box, IMSS will not label any email messages that violate this rule as spam. You can, however, still take actions on any senders in the Blocked Senders list below.
4. Select one of the following spam catch rates or specify a detection threshold.
   - **High:** Catches more spam. Select a high catch rate if too much spam is getting through to your clients.
   - **Medium:** Catches an average amount of spam (the default selection).
   - **Low:** Catches less spam. Select a low catch rate if IMSS is tagging too many legitimate email messages as spam.
   - **Specify a detection threshold:** Specify a threshold value (between 3.0 and 10.0) that represents how critically IMSS analyzes email messages to determine if they are spam.

Note: A higher threshold value means that a message must be very "spam-like" for IMSS to consider it spam. This decreases the spam catch rate, but it also results in a lower number of false positives. If IMSS is tagging too many legitimate email messages as spam (too many false positives), specify a higher threshold value.

A lower threshold value means that a message only needs to be slightly "spam-like" for IMSS to consider it spam. This increases the spam catch rate, but it also results in a higher number of false positives. If IMSS is letting too much spam through to your clients as legitimate email, specify a lower threshold value.

---

5. Click **DKIM approved list**, to enable or disable use of the DKIM Approved List. IMSS does not scan or mark messages as spam, if the messages come from domains appearing in the DKIM approved list
6. Select the check boxes next to any of the following lists to enable them:
   - **Approved sender list:** Prevents IMSS from identifying email from senders in this list as spam.

- **Blocked sender list:** Forces IMSS to identify email from senders in this list as spam.
- **Text exemption list:** Prevents IMSS from identifying email that contains any of the text in this list as spam.

Note: For instructions on configuring the lists, see Configuring Approved and Blocked Sender Lists on page 3-43.

---

7. Click **Save** to continue selecting scanning conditions.

Configuring Approved and Blocked Sender Lists

To provide added flexibility to spam filtering scanning conditions, IMSS provides the following lists:

- **Approved sender list:** Prevents IMSS from identifying email from senders in this list as spam.
- **Blocked sender list:** Forces IMSS to identify email from senders in this list as spam.

Configure the lists when you select spam scanning conditions.

To configure the approved or blocked sender lists:

1. Select the check box next to **Approved sender list** or **Blocked sender list**.
2. To add addresses manually, do the following:
   a. Next to **Email address**, type the address. To add multiple addresses, use the asterisk (*) wildcard.
   b. Click **Add**. The address appears in the list.
3. To import an address group from a file on a local host to the IMSS server, do the following:
   a. Click **Import**.
   b. Click **Browse** and locate the file. A dialog box appears.
   c. Click **Open**.
   d. If addresses are already in the list, choose whether to merge them or overwrite them with the imported list.

e. Click **Import**.

4. To export an address group as a file on the IMSS server, do the following:
   a. Click **Export**. A Save dialog box appears.
   b. Click **Save**.
   c. Specify a name for the file and a location to save the file.
   d. Click **Save**. The file saves to the location and a dialog appears.
   e. Click **Close**.
5. Click **Save**.

Configuring Spam Text Exemption Rules

IMSS does not identify any of the text in the text exemption list as spam. Configure rules for this list if you want users to always receive email messages that contain specific keywords.

Use regular expressions to define the conditions. Type a backslash character before any of the following characters:

\ | ( ) { } ^ $ * + . ?

To configure spam text exemption rules:

1. When configuring the spam scanning conditions, select the **Exclude messages matching text exemption rules** check box under **Text Exemption Rules**.
2. To add a new text exemption rule, click **Add**. To configure an existing rule, click it in the list box, and then click **Edit**. The Text Exemption Rules screen appears.
3. Next to **Name**, type a descriptive name for the text exemption rule.
4. Next to **Scan area**, select a portion of the email message.

Note: If you select **Subject**, **From**, **To**, or **Reply-to** as the scan area and use **Line beginning** to match the header, provide only the header content for **Line beginning**.

Example:
1. Select **From** as the scan area.
2. Under **Strings to match**, provide a message string for **Line beginning**. For example, **test@trendmicro.com**

If you select **All Headers** as the scan area and use **Line beginning** to match the header, provide the header name as well.

Example:
1. Select **All Headers** as the scan area.
2. Under **Strings to match**, provide both the header name and a message string for **Line beginning**. For example, **From: test@trendmicro.com**

5. Next to **Items are case sensitive**, select the check box to consider the text case as well as the content.
6. Under **Strings to match**, type the text strings in the text boxes. Line beginning means matching regular expressions at the beginning of a line. Line end means matching regular expressions at the end of a line.
7. Click **Save**.

Configuring Web Reputation Settings

Enable and configure Web Reputation settings to protect your clients from malicious URLs in email messages.

To enable Web Reputation:

1. Create or modify an "Other" (not an Antivirus) policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. Under Web Reputation on the Scanning Conditions screen, select the **Web Reputation settings** check box.

3. Click **Next** to continue configuring the policy.

To configure Web Reputation settings:

1. Create or modify an "Other" (not an Antivirus) policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
2. Under Web Reputation on the Scanning Conditions screen, click **Web Reputation settings**. The Web Reputation Settings screen appears.
3. Select one of the following catch rates or specify a detection threshold.
   - **High:** Blocks more Web sites embedded in email messages. Select a high sensitivity level if your clients are visiting too many malicious Web sites.
   - **Medium:** Blocks an average amount of Web sites (the default selection).
   - **Low:** Blocks fewer Web sites embedded in email messages. Select a low sensitivity level if IMSS is blocking too many legitimate Web sites embedded in email messages.
4. Select the **Enable the use of the Web Reputation Approved List** check box to bypass scanning and blocking of domains in the Web Reputation Approved List.
5. Click **Save** to continue selecting scanning conditions.

Selecting Scanning Conditions for Attachments

IMSS can filter email traffic based on the files attached to messages. Attachment scanning conditions include:

Scanning conditions for attachment names or extensions:

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **Name or extension**.
2. Click **Name or extension**. The Attachment Name or Extension screen appears.
3. Next to **Select**, select one of the following:
   - **Selected attachment names:** IMSS takes action on email messages with attachments of the selected names.
   - **Not the selected attachment names:** IMSS takes action on email messages with attachments that are not of the selected names.

4. Select the check boxes next to the attachments to scan or not scan.
5. To add your own attachment name, do the following:
   a. Select the check box next to **Attachments named**.
   b. Click **Import** to import from an existing text file. Another window appears.

      Alternatively, type the names in the text box. Use a semicolon (;) to separate values. You can also use an asterisk wildcard for the extension.

   c. Click **Save**.
6. Click **Save** to continue selecting scanning conditions.

Select MIME content type scanning conditions:

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **MIME content type**.
2. Click **MIME content type**. The Attachment MIME Type screen appears.
3. Next to **Select**, select one of the following:
   - **Selected attachment types:** IMSS takes action on email messages with attachments of the selected types.
   - **Not the selected attachment types:** IMSS takes action on email messages with attachments that are not of the selected types.
4. Select the check boxes next to the MIME content types to filter.
5. To add your own MIME types, type them in the text box. Use a semicolon (;) to separate values. You can also use an asterisk wildcard for the MIME type.
6. Click **Save** to continue selecting scanning conditions.

Select true file type scanning conditions:

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **True file type**.
2. Click **True file type**. The Attachment True File Type screen appears.
3. Next to Select, select one of the following:
   - **Selected attachment types:** IMSS takes action on email messages with attachments of the selected types.
   - **Not the selected attachment types:** IMSS takes action on email messages with attachments that are not of the selected types.
4. Select the check boxes next to the true file types to filter.

5. Click **Save** to continue selecting scanning conditions.

Select attachment size scanning conditions:

1. Under **Attachment** on the scanning conditions screen, select the check box next to **Size is {>, <, =} {size} {MB, KB, B}**.
2. Choose the comparison symbol (**>, <, =**).
3. Type a number to represent the size.
4. Choose Megabytes, Kilobytes, or Bytes (**MB, KB, B**).
5. Continue selecting scanning conditions.

Select attachment number scanning conditions:

1. Under **Attachment** on the scanning conditions screen, select the check box next to **Number is {>, <, =} {number}**.
2. Choose the comparison symbol (**>, <, =**).
3. Type a number to represent the number of attachments.
4. Continue selecting scanning conditions.

Select to block password protected files:

1. Under **Attachment** on the scanning conditions screen, select the check box next to **Password protected zip files**.

Selecting Scanning Conditions for Message Size

IMSS can take action on an email message based on its total size, including all attachments.

To select message size scanning conditions:

1. Under **Size** on the scanning conditions selection screen, select the check box next to **Message size is {>, <, =} {size} {MB or KB}**.
2. Choose the comparison symbol (**>, <, =**).
3. Type a number to represent the size of the email message.
4. Choose **Megabytes** or **Kilobytes** (**MB** or **KB**).
5. Continue selecting scanning conditions.

Selecting Scanning Conditions for Message Content

IMSS can take action on an email message based on its content and where the content appears. See Configuring an Expression on page 3-15 for more information on how to specify the content to filter.

To select scanning conditions for content:

1. Click **Policy > Policy List**. The Policy screen appears.
2. Create or modify an "Other" (not an Antivirus) policy.
3. Under **Content**, on the Step 2: Select Scanning Conditions screen, select the check boxes next to the parts of an email message to which you want the content conditions to apply.
4. Click the link that specifies the part of the email message to which you want to configure content conditions. The Keyword Expressions screen appears with two columns:
   - **Available:** Expressions available for use, but not currently in use.
   - **Selected:** Expressions currently in use.
5. If you are configuring expressions for the header, select the check boxes next to the header items where the expression will apply.
6. Click **Add**. The screen for managing keyword expressions appears.
7. Configure the expressions.
8. In the **Available** list, click the expression list you want to enable.
9. Click **>>**. The expressions appear in the Selected list.

   To keep an expression list available but temporarily prevent IMSS from using it, click the expression in the selected list, and then click **<<**.
10. Click **Save** to continue to the scanning conditions selection screen.

Specifying "Other" Scanning Conditions

IMSS can filter email traffic based on the following:

- Number of recipients
- Message arrival time
- Message content is encrypted

To specify "Other" scanning conditions:

1. Click **Policy > Policy List**. The Policy screen appears.
2. Create or modify an "Other" (not an Antivirus) policy.
   - For information on creating a new rule, see Adding Policies on page 3-29.
   - For information on modifying an existing rule, see Modifying Existing Policies on page 3-61.
3. Under **Other**, on the Scanning Conditions screen, select the check boxes next to the following:
   - **Number of recipients {>, <, =} {number}:** Blocks messages if the number of recipients is less than, exceeds, or is equal to the specified limit.
   - **Received time range:** Blocks messages if they enter your network within the specified time range
   - **Encrypted messages:** Blocks encrypted messages that cannot be scanned by IMSS.

Selecting Scanning Conditions for Number of Recipients

IMSS can take action on an email message based on the number of recipients to which the message is addressed.

To select recipient number scanning conditions:

1. Under **Others** on the scanning conditions selection screen, select the check box next to **Number of recipients {>, <, =} {number}**.
2. Choose the comparison symbol (**>, <, =**).
3. Type a number to represent the number of recipients.
4. Continue selecting scanning conditions.

Setting Scanning Conditions for Message Arrival Time

IMSS can take action on an email message based on the time it arrived.

To select time range scanning conditions:

1. Under **Others** on the scanning conditions selection screen, select the check box next to **Received time range**.
2. Click **Received time range**. The Time Range screen appears.

3. Next to **Select**, choose one of the following:
   - **Anytime within selected ranges**
   - **Anytime except selected ranges**
4. From the time drop-down boxes, select the day, start time, and end time.
5. Click **Add**.
6. Click **Save** to continue selecting scanning conditions.

Specifying Actions

The main actions for both the Antivirus and Other rules are similar, although there are minor differences in the options listed. Select the desired action(s) from the following categories:

- **Intercept**: Allows you to choose whether you would like IMSS to intercept the messages and prevent them from reaching the recipients. Choosing the intercept option allows you to specify an action for IMSS to take on intercepted messages.
- **Modify**: Instructs IMSS to make some alterations to the messages or the attachments, such as inserting a stamp or tagging the subject.
- **Monitor**: Instructs IMSS to send a notification, archive or blind copy the messages if you would like to further analyze them.

To set the actions:

1. Click **Next** from the Step 2: Select Scanning Conditions screen. The Step 3: Select Actions screen appears.

Note: The user interface that appears in this step depends on the type of rule that you are creating. The antivirus rule contains two tabs that allow you to configure the main actions and the actions for special viruses.

Specify actions for "Other" rules:

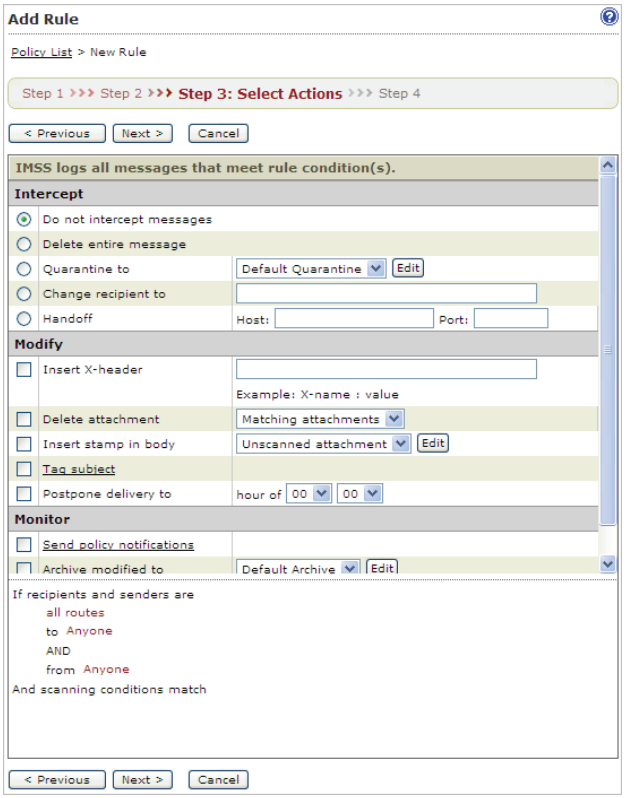


FIGURE 3-2. Other Rule Actions

1. Under **Intercept**, click the radio button next to one of the following:
   - **Do not intercept messages:** This specific rule does not intercept messages. If there are other rules, IMSS will process the message. If there are no rules, IMSS passes the message to your network.
   - **Delete entire message:** Deletes the message and all attachments.

- **Quarantine:** IMSS puts the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see Configuring Quarantine and Archive Settings on page 5-26.
- **Change recipient:** IMSS sends the message to another recipient. Type the recipient email address and separate multiple recipients with a semicolon (;).
- **Handoff:** IMSS hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
  - Next to **Host**, type the FQDN or IP address of the mail server.
  - Next to **Port**, type the port number through which the mail server receives email traffic.

Note: IMSS can only track a message before it is handed off. After the handoff, the message is not traceable anymore as it is no longer within the control of IMSS.

---

2. Under **Modify**, select the check boxes next to any of the following:
   - **Insert X-header:** Inserts a user-specified message to the header of email messages.
   - **Delete attachments:** Select an action for IMSS to take:
     - **Delete matching attachment:** Remove only the attachment that matches the attachment scan condition.
     - **Delete all attachments:** Remove all attachments.
   - **Insert stamp in body:** Insert text at the beginning or end of the message. From the drop down box, select the name of the stamp to insert or click **Edit** to go to the Stamps screen and manage your stamps.
   - **Tag subject:** Add text to the subject line of the message. Click **Tag subject** to edit the tag.
   - **Postpone delivery time:** Delay delivery until a specified hour of the day. Select the hour of the day and minutes from the drop down boxes.
3. Under **Monitor**, select the check boxes next to any of the following:

- **Send policy notifications:** Send an email message to one or more recipients. To select a type of notification, click **Send policy notifications**. For instructions on creating notifications, see Using the Notifications List on page 3-17.
- **Archive modified to:** Archive the message to an archive area. For instructions on creating a new archive area, see Configuring Quarantine and Archive Settings on page 5-26.
- **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

Specify actions for "Virus" rules Main Actions:

Main Actions allow you to specify the default actions that IMSS takes when messages match the scanning conditions specified in Step 2: Scanning Conditions.

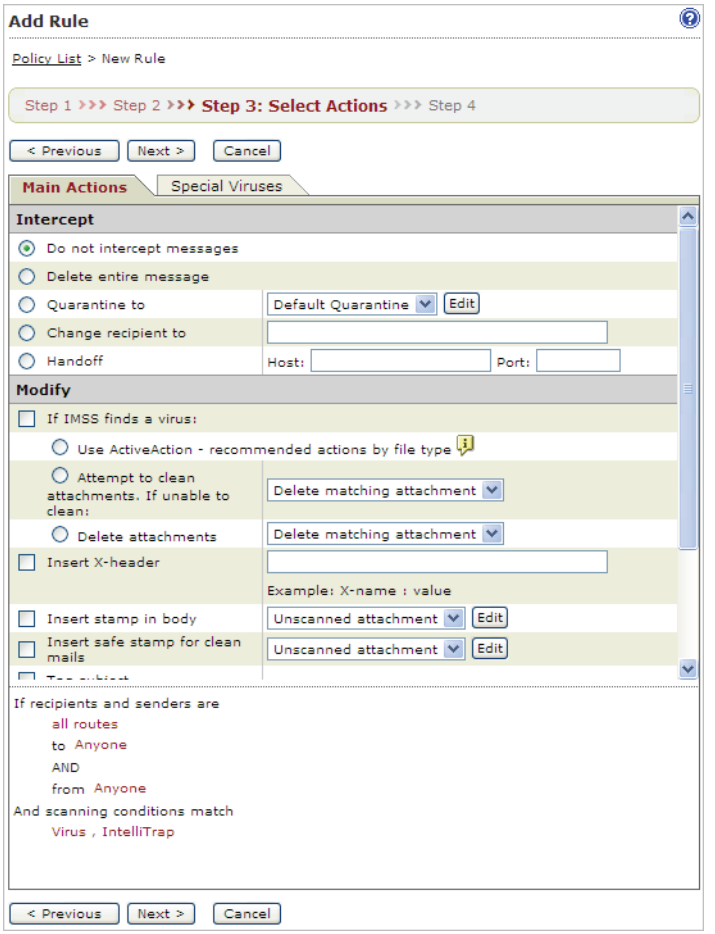


FIGURE 3-3. Antivirus Rule Main Actions

1. Under **Intercept**, click the radio button next to one of the following:
   - **Do not intercept messages:** This specific rule does not intercept messages. If there are other rules, IMSS will process the message. If there are no rules, IMSS passes the message to your network.
   - **Delete entire message:** Deletes the message and all attachments.

- **Quarantine:** IMSS puts the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see Configuring Quarantine and Archive Settings on page 5-26.
- **Change recipient:** IMSS sends the message to another recipient. Type the recipient email address and separate multiple recipients with a semicolon (;).
- **Handoff:** IMSS hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
  - Next to **Host**, type the FQDN or IP address of the mail server.
  - Next to **Port**, type the port number through which the mail server receives email traffic.

Note: IMSS can only track a message before it is handed off. After the handoff, the message is not traceable anymore as it is no longer within the control of IMSS.

2. Under **Modify**, select the check boxes next to any of the following:

Note: Options under **If IMSS finds a virus** are only available for Antivirus rules.

- **If IMSS finds a virus:** Select the check box to enable actions if IMSS finds a virus or other malware, and then click one of the following:
  - **Use ActiveAction:** Enable IMSS to automatically use preconfigured scan actions for specific types of viruses/malware.
  - **Attempt to clean attachments. If unable to clean:** Select an action for IMSS to take if it cannot clean the attachment:
    - **Delete matching attachment:** Remove only the attachments with viruses/malware.
    - **Delete all attachments:** Remove all attachments.
  - **Delete attachments:** Select an action for IMSS to take:
    - **Delete matching attachment:** Remove only the attachment with viruses/malware.
    - **Delete all attachments:** Remove all attachments.

- **Insert X-header:** Inserts a user-specified message to the header of email messages.

Note: If you configure multiple rules to add an x-header, the x-header appears only once in the message. The x-header appears as configured in last rule.

- **Insert stamp in body:** Insert text at the beginning or end of the message. From the drop down box, select the name of the stamp to insert or click **Edit** to go to the Stamps screen and manage your stamps.
- **Insert safe stamp for clean mails:** Insert text into clean emails signifying that the email is safe. From the drop down box, select the name of the stamp to insert or click **Edit** to go to the Stamps screen and manage your stamps.

Note: The **Insert safe stamp for clean mails** option is not available on the Special Viruses tab.

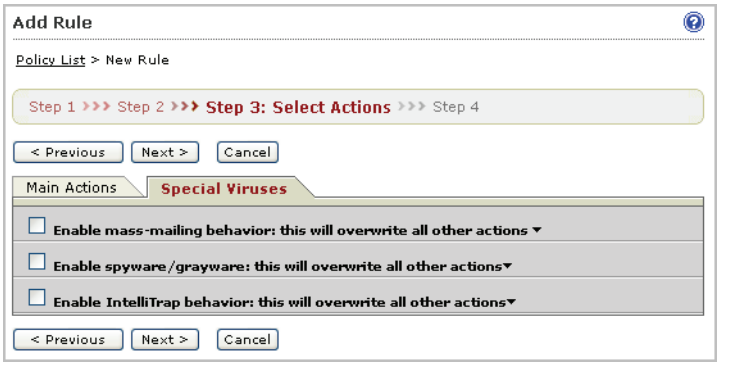
- **Tag subject:** Add text to the subject line of the message. Click **Tag subject** to edit the tag.
- **Postpone delivery time:** Delay delivery until a specified hour of the day. Select the hour of the day and minutes from the drop down boxes.

3. Under **Monitor**, select the check boxes next to any of the following:
   - **Send policy notifications:** Send an email message to one or more recipients. To select a type of notification, click **Send policy notifications**. For instructions on creating notifications, see Using the Notifications List on page 3-17.
   - **Archive modified to:** Archive the message to an archive area. For instructions on creating a new archive area, see Configuring Quarantine and Archive Settings on page 5-26.
   - **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

Specify actions for "Virus" rules Special Viruses:

Special Virus settings allow you to specify the actions that IMSS takes if the messages match any of the following criteria. The actions specified on this screen will override the default actions specified on the Main Actions tab.

Note: These options are only available for Antivirus rules.



- **Mass mailing:** IMSS takes the actions specified in this section if it detects mass mailing messages.
- **Spyware/grayware:** Allows you to specify the corresponding actions if you have selected any of the Spyware/Grayware Scanning options on the Scanning Conditions screen in step 2. For more information, see Specifying Scanning Conditions on page 3-36. If IMSS detects spyware/grayware in a message, it takes the actions that are specified here.

  Note: IMSS takes the default action for messages matching the Spyware/Grayware Scanning conditions if you do not select alternative actions.

- **IntelliTrap:** Allows you to specify the corresponding actions if you have selected the IntelliTrap Setting options on the Scanning Conditions screen in step 2. See Specifying Scanning Conditions on page 3-36.

Note: IMSS takes the default action for messages matching the IntelliTrap conditions if you do not select alternative actions.

Creating a Tag Subject

To notify a recipient that IMSS took action on a message's attachment or that the message violated scanning conditions for a rule, add a brief message to the beginning of the subject line. Add a tag only for email that the intended recipients will eventually receive. If you are configuring a rule to delete messages that violate your scanning conditions, adding a tag is not necessary.

To add a tag:

1. When you select actions, click **Tag subject** under Modify actions. An edit screen appears.
2. Next to Tag, type the text to insert in the subject line.
3. To prevent possible damage to digitally signed messages, select **Do not tag digitally signed messages**.
4. Click **Save** to continue selecting actions.
5. To use tag, select the check box next to **Tag subject** under Modify.

Finalizing a Policy

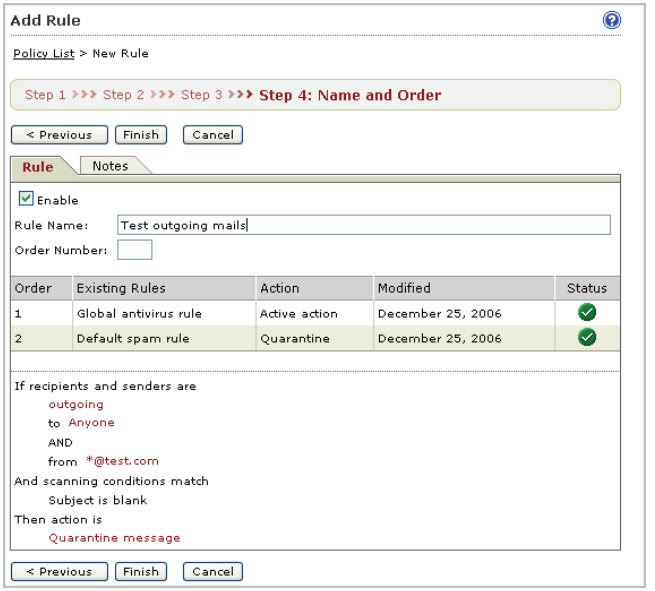
After you select actions for a rule, name and enable the rule. Also, assign an order number that represents its position within the hierarchy of rules. IMSS allows you to add any notes to the rule that you think are necessary for future reference. You can also modify this information for an existing rule.

When viewing rules, be aware of the following:

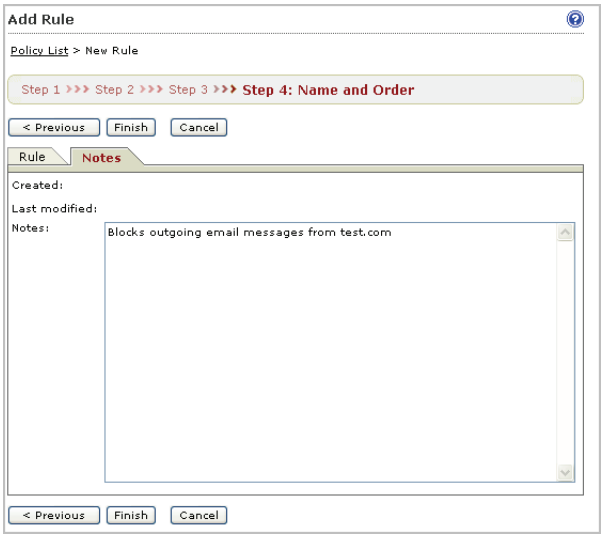
-  A green check mark represents active rules.
-  A red X symbol represents rules that are saved but inactive.
-  A gray X symbol represents that the rules and the Activation Code for the product are inactive.

To finalize a rule:

1. Use one of the following methods to open the screen:
   - When creating a new policy, click **Next** on the Step 3: Select Actions screen. The Step 4: Name and Order screen appears.
   - When finalizing an existing policy, click the name of the policy in the policy list on the **Policy > Policy List** screen



2. Select the **Enable** check box to activate the rule.
3. Type a name for the rule in the **Rule Name** field.
4. In the **Order Number** field, specify the priority in which IMSS will perform the scan. IMSS applies the rule to messages according to the order you specify.
5. Click the **Notes** tab. The Notes screen appears.



6. Type a note to distinguish the new rule from other rules.
7. If you are creating a new policy, verify that the information on the screen is correct. If any information about the rule is incorrect, click **Previous** and make your changes.
8. Click **Finish** to complete a new rule or **Save** to modify an existing rule.

Modifying Existing Policies

Modification of rules follows a different process from rule creation.

To modify existing rules:

1. Choose **Policy > Policy List** from the menu.
2. Click the name of the rule to edit. The Summary screen for the rule appears.
3. Click **Edit** for **If recipients and senders are**.
4. Configure the route settings. For more information, see Specifying a Route on page 3-29.
5. Click **Edit** for **And scanning conditions match** or **And domains listed here do not pass DKIM verification**.

6. Configure the scan settings. For more information, see the following:
   - For Antivirus and Other rules: Specifying Scanning Conditions on page 3-36
   - For the Global DKIM Enforcement rule: Using the Domain List for the Global DKIM Enforcement Rule on page 3-62
7. Click **Edit** for **Then action is**.
8. Configure the action settings. For more information, see Specifying Actions on page 3-51.
9. Click **Save**.

Using the Domain List for the Global DKIM Enforcement Rule

IMSS marks incoming messages from domains appearing in the Domain List, that do not pass DKIM validation or do not have a DKIM-Signature, as spam.

To add domains to the Domain List in the Global DKIM Enforcement rule:

1. Click **Policy > Policy List**. The Policy screen appears.
2. Click the **Global DKIM Enforcement rule** link. The Policy Summary screen appears.
3. Click **Edit** in the **And domains listed here do not pass DKIM verification** row. The Scanning Conditions screen appears.
4. Populate the Domain List in one of the following ways:

   Manually:

   a. Type a domain name.

   b. Click **Add**.

   Import a list:

   Note: When importing a text file for the Domain List, only one domain should be on each line.

   a. Click **Import**. The Import DKIM Enforcement List appears.

   b. Type the file path and file name or click **Browse** and locate the file.

   c. Select one of the following:

      - **Merge with current list**

- **Overwrite current list**

d. Click **Import**.

5. Click **Save**.

Policy Example 1

Create a rule to delete attachments with specific file names or extensions and then stamp the affected incoming message with an explanation to the recipients.

Step 1: Specify the Route

1. Choose **Policy** > **Policy List** from the menu.

2. Click **Add**.

3. Select **Other** from the drop-down list. The Step 1: Select Recipients and Senders screen appears.

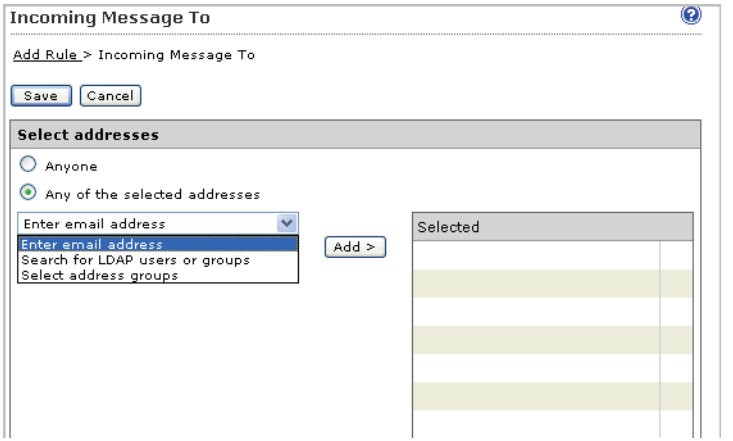
4. Next to **This rule will apply to**, select **incoming messages** from the drop-down list.

5. Click the **Recipients** link. The Select addresses screen appears.

a. To apply this rule to any recipients, select **Anyone**.

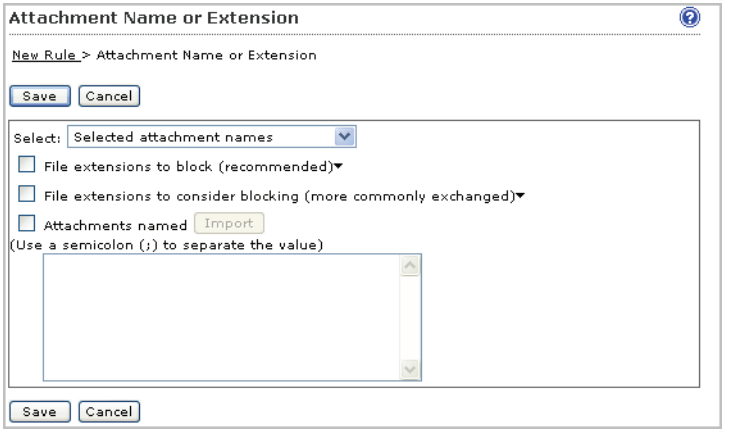
b. To apply this rule to specific recipients, choose **Any of the selected addresses**, and then specify the target email address or group.

c. Click **Save**. The Step 1: Select Recipients and Senders screen re-appears.



Step 2: Specify the Scanning Conditions

1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Name or extension** condition, select the check box next to it.
4. Click **Name or extension**. The Attachment Name or Extension screen appears.

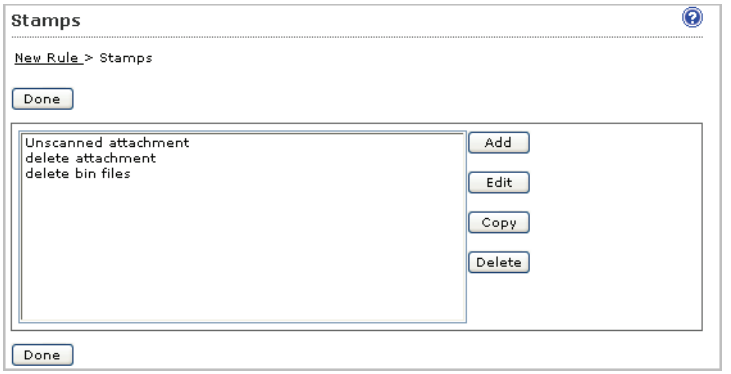


5. Select the file extensions to block or consider blocking.

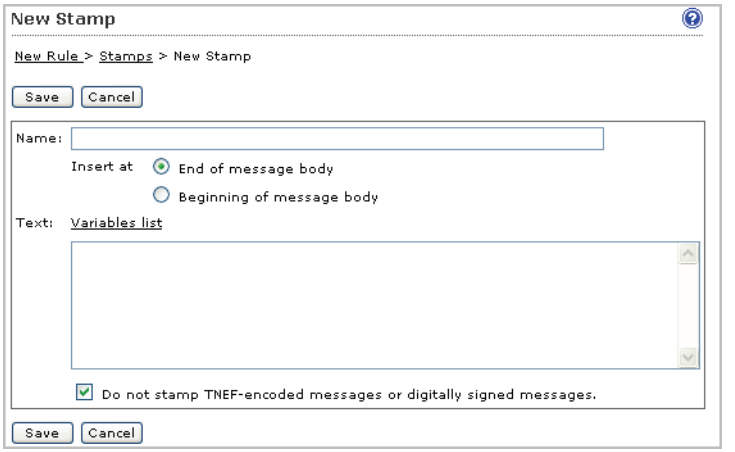
6. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears.

Step 3: Specify the Actions

1. Click **Next**. The Step 3: Select Actions screen appears.
2. Under **Modify**, to enable the **Delete attachment** action, select the check box next to it.
3. Select **Matching attachment** from the drop-down list if it is not already selected.
4. Select the check box next to **Insert stamp in body.**
5. If there is no suitable stamp available from the drop-down list, click **Edit**. The Stamps screen appears.



6. Click **Add** to create a new stamp. The New Stamp screen appears.



7. Provide the required information.
8. Click **Save**. The Stamps screen re-appears.
9. Click **Done**. The Select Actions screen re-appears.
10. Select the newly created stamp from the drop-down list.

Step 4: Specify the Priority

1. Click **Next**. The Step 4: Name and Order screen appears.
2. Type the rule name and order number.
3. Click **Finish**. The newly created rule will appear highlighted in the Policy list screen.

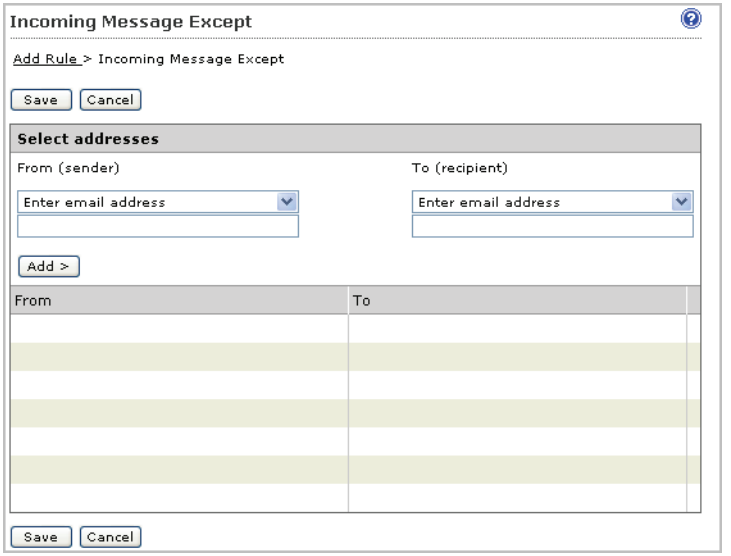
Policy Example 2

Create a rule that quarantines messages containing specific keywords in the subject or body and then apply this rule to all recipients except administrators.

Step 1: Specify the Route

1. Choose **Policy** > **Policy List** from the menu. The Policy List screen appears.
2. Click **Add**.

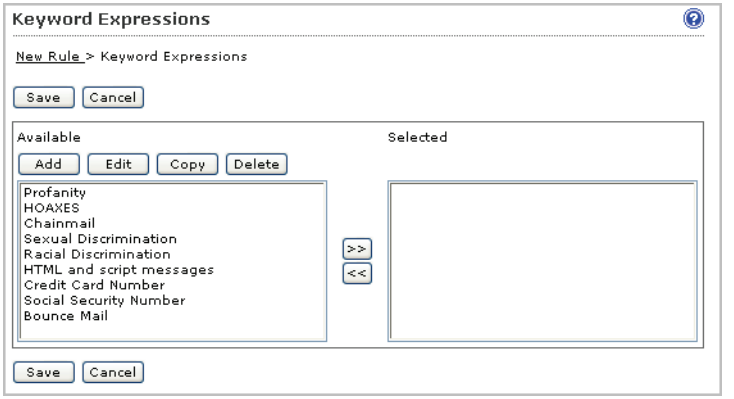
3. Select **Other** from the drop-down list. The Step 1: Select Recipients and Senders screen appears.
4. Next to **This rule will apply to**, select **incoming messages** from the drop-down list.
5. Click the **Recipients** link. The Select addresses screen appears.
6. Select **Anyone**.
7. Click **Save**. The Step 1: Select Recipients and Senders screen re-appears.
8. Click the **Sender to Recipient link** next to **Exceptions**. The Exceptions screen appears.



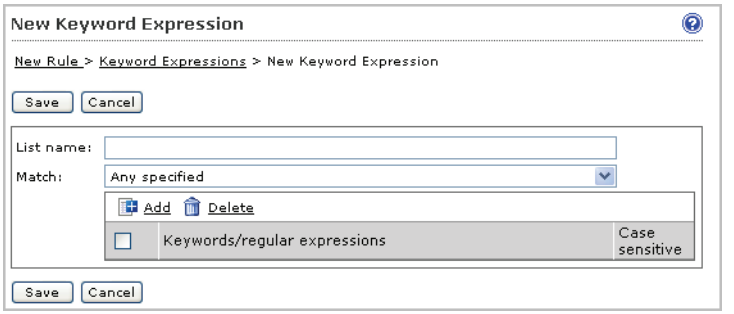
9. Under **From (sender)**, type ***@*** to specify any sender.
10. Under **To (recipient)**, type the administrator's email address.
11. Click **Add**. The sender-recipient pair appears in the list.
12. To add other administrators or recipients, repeat steps 9 to 11.
13. Click **Save** after you finish adding all the desired recipients. The Step 1: Select Recipients and Senders screen re-appears.

Step 2: Specify the Scanning Conditions

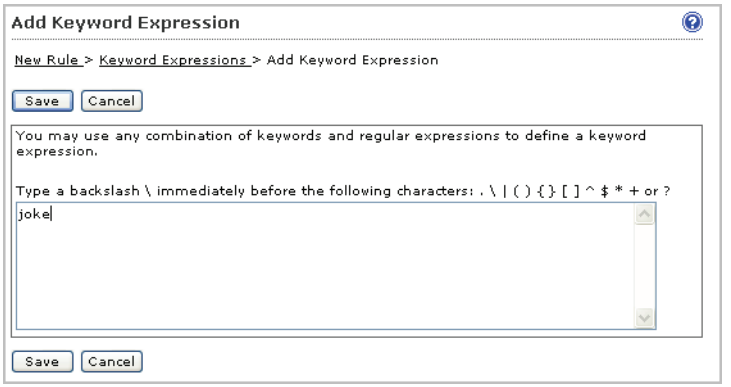
1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Subject Keyword Expressions** condition under **Content**, select the check box next to it.
4. Click **Subject Keyword Expressions**. The Keyword Expressions screen appears.



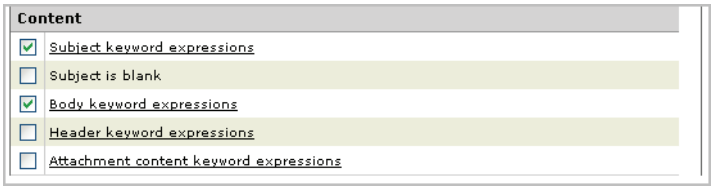
5. If the desired keywords are not available from the existing list, click **Add** to create a new keyword list. The New Keyword Expression screen appears.



6. Specify the required information.
7. To add an individual keyword expression, click **Add**. The Add Keyword Expressions screen appears.



8. Type the desired keyword expression and click **Save**. The New Keyword Expression screen re-appears.
9. Repeat steps 7 and 8 for additional keyword expressions.
10. After you have added all the required keyword expressions, type the **List name** for the new keyword list and click **Save**. The Keyword Expressions screen re-appears with the newly created keyword list.
11. Select the new list and click **>>** to insert the list into the Selected box.
12. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears.
13. To enable the **Body Keyword Expression** condition**,** select the check box next to it.
14. Click **Body Keyword Expression**. The Keyword Expressions screen appears.
15. Select the new keyword list and click **>>** to insert the list into the Selected box.
16. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears. Ensure that both the Subject keyword and Body keyword expressions are selected.



Step 3: Specify the Actions

1. Click **Next**. The Step 3: Select Actions screen appears.
2. Under **Intercept**, select **Quarantine to**.
3. Accept the **Default Quarantine** area or click the drop-down list to select the desired quarantine area.

Step 4: Specify the Priority

1. Click **Next**. The Step 4: Name and Order screen appears.
2. Type the rule name and order number.
3. Click **Finish**. The newly created rule will appear highlighted in the Policy list screen.

Using the Asterisk Wildcard

You can use the asterisk (*) as a wildcard in email addresses when defining routes and in file names.

Wildcards in Email Addresses

Wildcards can appear in the name or domain sections of an email address. The following are valid examples:

- ***@*:** Valid representation of all email addresses.
- ***@domain.tld, name@*.tld:** Valid representation of the whole name or the domain (not the top level domain (TLD)).
- ***@*.tld:** Valid representation of both the name and the domain (not the TLD).

Wildcards cannot appear in a subdomain or the top-level domain. Wildcards also cannot appear with other letters; they must appear alone. The following are invalid examples:

- **name@domain.*.tld:** Invalid representation of a subdomain.
- **name@domain.*:** Invalid representation of a TLD.
- ***name@domain.tld:** Invalid use in conjunction with a name.

Wildcards in File Names

You can use wildcard characters in file names the same way you can use them in email addresses. Use an asterisk in the name or the extension sections of a filename, but not in conjunction with a partial name or extension. The following are valid examples:

- ***.*:** Valid representation of all files.
- ***.extension:** Valid representation of all files of a certain extension.
- **name.*:** Valid representation of files with a specific name but with any extension.

The following are invalid examples:

- ***name.*:** Invalid representation of a name.
- **name.*extension:** Invalid representation of an extension.

Setting Scan Exceptions

Under certain circumstances, you may want to prevent IMSS from scanning certain types of email messages that could be part of a DoS attack. For example, messages with extremely large attachments require significant IMSS server resources to scan fully. Additionally, messages addressed to hundreds of recipients are most likely spam or some type of attack.

Rather than consuming IMSS resources to scan these types of email messages, set scan exceptions to bypass scanning and instruct IMSS to take action on the messages immediately.

WARNING! **1. For the actions specified in Scan Exceptions take effect, verify that the Global antivirus rule is enabled.**

2. For malformed messages, when a message triggers the scan exception, IMSS stops scanning and takes the corresponding actions. That means IMSS will not trigger any policy rules when a scan exception occurs.

For security setting violation, IMSS will not stop scanning after the action of the scan exception executes. IMSS continues checking other policy rules.

To configure scan exceptions:

1. Choose **Policy > Scanning Exceptions** from the menu.
2. To set scan exception conditions for email messages based on several conditions, click the Security settings violations link under Exception. The Security Settings Violations screen appears, where you can configure the settings.
3. To set an action for an exception type, click the corresponding link under Action:
   - Setting Scan Actions for Security Setting Violations on page 3-73
   - Setting Scan Actions for Malformed Messages Scanning Exceptions on page 3-74

Configuring Exceptions for Security Settings Violations

The scan exceptions for the security settings violations on this screen apply to all senders and receivers.

To configure security settings violations:

1. On the Scanning Exceptions screen, click **Security settings violations** under **Exception**. The Security Settings Violations screen appears.
2. To set limits on the types of email messages IMSS can scan, configure the following:
   - **Total message size exceeds { } MB:** Type the maximum number of megabytes.
   - **Total # recipients exceeds { } recipients:** Type the maximum number of recipients.

- **Total # embedded layers in compressed file exceeds { } layers:** Select the maximum number of layers.
- **Total decompressed size of any single file exceeds { } MB:** Type the maximum number of megabytes.
- **Total # files in compressed file exceeds { } files:** Type the maximum number of files.

3. Click **Save**. The Scanning Exceptions screen reappears.

Setting Scan Actions for Security Setting Violations

To set scan actions for security settings violations:

1. On the Scanning Exceptions screen, click the action name link under **Actions** for **Security settings violations**. The screen for configuring actions appears.
2. Under **Intercept**, click the radio button next to one of the following:
   - **Do not intercept messages:** IMSS does not take action on the message. IMSS processes the message using other rules if other rules exist.
   - **Delete entire message:** Deletes the message and all attachments.
   - **Quarantine to:** IMSS moves the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see Configuring Quarantine and Archive Settings on page 5-26.
   - **Handoff:** IMSS hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
     - Next to **Host**, type the FQDN or IP address of the mail server.
     - Next to **Port**, type the port number through which the mail server receives email traffic.

Note: IMSS can only track a message before it is handed off. After the handoff, the message is not traceable anymore as it is no longer within the control of IMSS.

---

3. Under **Monitor**, select the check boxes next to any of the following:

- **Send policy notifications:** Send a notification message to one or more recipients. To select a type of notification, click **Send policy notifications**. For instructions on creating notifications, see Using the Notifications List on page 3-17.
- **Archive:** Archive the message to an archive area. For instructions on creating a new archive area, see Configuring Quarantine and Archive Settings on page 5-26.
- **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

4. Click **Save**.

Setting Scan Actions for Malformed Messages Scanning Exceptions

To set scan actions for malformed messages scanning exceptions:

1. On the Scanning Exceptions screen, click the action name link under **Actions** for **Malformed messages**. The screen for configuring actions appears.
2. Under **Intercept**, click the radio button next to one of the following:
   - **Do not intercept messages:** IMSS does not take action on the message. IMSS passes the message on for delivery.

Note: IMSS does not scan malformed messages with other rules, even if other rules exist.

   - **Delete entire message:** Deletes the message and all attachments.
   - **Quarantine to:** IMSS moves the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see Configuring Quarantine and Archive Settings on page 5-26.
   - **Handoff:** IMSS hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
     - Next to **Host**, type the FQDN or IP address of the mail server.

- Next to **Port**, type the port number through which the mail server receives email traffic.

Note: IMSS can only track a message before it is handed off. After the handoff, the message is not traceable as it is no longer within the control of IMSS.

3. Under **Monitor**, select the check boxes next to any of the following:
   - **Send policy notifications:** Send an email message to one or more recipients. To select a type of notification, click **Send policy notifications**. For instructions on creating notifications, see Using the Notifications List on page 3-17.
   - **Archive:** Archive the message to an archive area. For instructions on creating a new archive area, see Configuring Quarantine and Archive Settings on page 5-26.
   - **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.
4. Click **Save**.

Chapter 4

Backing Up, Restoring, and Replicating Settings

This chapter provides instructions on how to back up and restore IMSS configuration settings. If you have deployed multiple IMSS scanners and are using Trend Micro Control Manager simultaneously, you can also replicate IMSS settings without having to reconfigure settings for each new scanner.

Topics include:

Import/Export Settings

Use the Import/Export screen to create a backup of IMSS settings. Keeping a backup allows you to easily re-apply your settings to an IMSS 7.1 server. You can also replicate a configuration across several IMSS 7.1 servers by importing the same configuration file into the desired servers.

To export configuration files:

1. Choose **Administration > Import/Export** from the menu.
2. Click **Export**.
3. When the dialogue box appears, click **Save** and save it to your computer.
4. To return to the **Import/Export** screen, click **Return**.

During export, do not:

- Access other Web console screens or modify any settings.
- Perform any database operations.
- Start/stop any IMSS services.
- Register/unregister any EUQ database to/from IMSS
- Start other export or import tasks.

To import configuration files:

1. Log on to the IMSS Web console.
2. Choose **Summary** from the menu. Verify that no services are starting or stopping. If services are starting or stopping, wait until the operation has completed.
3. Choose **Administration > Import/Export** from the menu.
4. Under **Import Configuration Files**, click **Browse...** and locate the file.
5. Click **Import**. The original IMSS settings and rules, such as domain-based delivery settings, will be deleted and replaced by the imported settings and rules.

During import, do not:

- Access other Web console screens or modify any settings.
- Perform any database operations.
- Start/stop any IMSS services.
- Register/unregister any EUQ database to/from IMSS
- Launch other export or import tasks.

If the import fails, the configuration will roll back to the original settings before the import.

Backing Up IMSS

After you have installed IMSS and configured the required settings, it is always prudent to create backups of the settings so that you can restore IMSS quickly in the event of a system failure.

You can choose to perform a full or minimal backup of IMSS as follows:

- **Full:** Backs up all IMSS local configuration and binary files stored in `/opt/trend` and database-related files in `/var/imss`.
- **Minimal:** Backs up only IMSS configuration settings stored in `/opt/trend/imss/config`.

Note: 1. The backup and restore instructions in this manual are targeted at the all-in-one deployment of IMSS. In the case of distributed deployment, you need to back up the following:
a. The database files or tables on the computer(s) where you installed the databases.
b. The local binary and configuration files on every computer where you installed IMSS components.

2. If you perform a minimal backup, you may need to install previous hot fixes, patches, or service packs after restoring IMSS.

To perform a full backup:

1. Stop all IMSS-related processes:

   ```
   /opt/trend/imss/script/imssstop.sh stop
   ```

2. Stop Postfix.

3. Back up the folder `/opt/trend/ and /var/imss/`.
4. Back up all Postfix configuration files under `ect/postfix`. For example, `main.cf`, `master.cf`, `allowAccessList`, `denyAccessList`.
5. Start Postfix.
6. Start all IMSS-related processes:

   `/opt/trend/imss/script/imssstart.sh`

To perform a minimal backup:

1. Stop all IMSS-related processes. For details, see To perform a full backup: on page 4-3.
2. Stop Postfix.
3. Back up the `/opt/trend/imss/config` folder.
4. Back up the folder `ect/postfix`.
5. Back up all database tables.
6. Start Postfix.
7. Start all IMSS-related processes. For details, see To perform a full backup: on page 4-3.

Restoring IMSS

In the event of a system failure, you can restore IMSS depending on whether you have performed a full or minimal backup previously.

To perform full restoration:

1. Install a new IMSS server on one computer, ensuring that the IP address, database user name, and password are the same as the original.
2. Stop all IMSS-related processes. For details, see To perform a full backup: on page 4-3.
3. Stop Postfix.
4. Restore the folders `/var/imss/` and `/opt/trend/` using the previous backup.
5. Restore Postfix configuration files.
6. Start Postfix.

7. Start all IMSS-related processes. For details, see To perform a full backup: on page 4-3.

To perform minimal restoration:

1. Install a new IMSS server on one computer, ensuring that the IP address, database user name, and password are the same as the original.
2. Stop all IMSS-related processes. For details, see To perform a full backup: on page 4-3.
3. Stop Postfix.
4. Restore the `/opt/trend/imss/config/` folder using the previous backup.
5. Restore Postfix configuration files.
6. Import the previous database table backup into the new database.
7. Start all IMSS-related processes. For details, see To perform a full backup: on page 4-3.

Replicating Settings

If you have installed multiple IMSS scanners that do not share the same admin database, you can use Trend Micro Control Manager to replicate settings across these scanners without having to configure each scanner separately. If the scanners share the same admin database, it is not necessary to replicate settings.

Do the following if you intend to replicate settings using Control Manager:

Step 1. Back up IMSS settings. For details, see Backing Up IMSS on page 4-3.

Step 2. Enable the Control Manager agent.

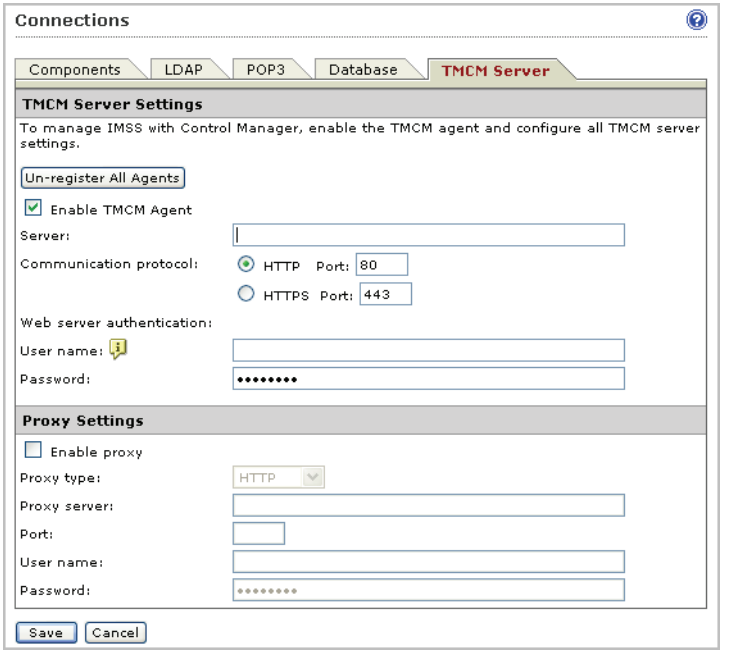
Step 3. Replicate settings from the Control Manager Web console.

Enabling Control Manager Agent

IMSS automatically installs the Trend Micro Management Communication Protocol agent during installation. To integrate with Control Manager, provide the Control Manager server details and enable the agent from the Web management console.

To configure Control Manager Server settings:

1. Choose **Administration** > **Connections** from the menu. The Components tab appears by default.
2. Click the **TMCM Server** tab. The TMCM Server Settings screen appears.



3. Provide the required information.
4. Select the check box next to **Enable TMCM Agent**.
5. Click **Save**.

Replicating Settings from Control Manager

After enabling the Management Communication Protocol agent from the IMSS Web management console, you can start to replicate IMSS settings by logging on to the Control Manager Web console.

To replicate IMSS settings:

1. Click **Products** from the Control Manager menu. The Product Directory screen appears.
2. Locate the source IMSS scanner from the Product Directory tree.
3. Mouseover **Configure**. A drop-down list appears.
4. Select **Configuration Replication** from the drop-down list.
5. Select the check box next to the target server.
6. Click the **Replication** button.

Chapter 5

Monitoring the Network

This chapter provides you with general instructions on the tasks that you need to perform for the day-to-day maintenance of IMSS. For more information on each field on the Web management console, refer to the Online Help.

Topics include:

Monitoring Your Network

IMSS provides a complete set of tools that enable you to monitor your network traffic. You can obtain useful information such as the statistics on the performance of IMSS components, or generate reports that display a breakdown of messages matching various scanning conditions.

Viewing Statistics Summary

The Statistics Summary screen shows the following information:

- **Performance Overview:** The incoming, outgoing, and total number of messages that IMSS processed. The processing speed is also displayed in messages per minute.
- **Scan Performance:** The scanning conditions that were violated. Message counts will overlap. The percentage in column refers to the total number of messages.
- **IP Filtering Performance:** The type of threat IMSS blocked using the IP filtering product.

To view the statistics:

1. Choose **Summary** from the menu.
2. Select the desired last # days/hours from the **Show** drop-down list.

Note: IMSS automatically updates these statistics in its database every hour at 15 minutes past the hour.

Viewing System Summary

The System Summary screen provides at-a-glance information about the status of IMSS components and services.

To view the System Summary:

1. Choose **Summary** from the menu.

   From the System Summary screen, you can manage the following:

- **Connections:** The connections currently enabled (POP3, ERS, and IP Profiler).

  To enable or disable connections:

  a. Select or clear the check box next to a connection item.

b. Click **Save**.

- **Components:** The version numbers of the antivirus, anti-spyware, and anti-spam components that IMSS uses to protect your network.

  To manually update components:

  a. Select the check box next to the component to update.

  b. Click **Update**.

  To roll back to the previous version of the components:

  a. Select the check box next to the component to roll back.

  b. Click **Rollback**.

  To refresh the page:

  - Click **Refresh** to connect to the update source and display the latest component versions in the Availability column.

- **Managed services:** Other IMSS services registered to this IMSS admin database.

  To start or stop managed server services:

  - Click **Start** or **Stop** under the service to change.

  To unregister managed server services:

  - When a managed service is inactive (it is disconnected from the IMSS server), the Remove button will appear in the Connection column next to the specific service. To remove the managed service from this IMSS server, click **Remove**.
  - A managed service could become disconnected for any of the following reasons:
    - You removed the scanner.
    - The IMSS manager service stopped.
    - The scanner server is shut down.

Interpreting the Statistics

IMSS presents performance statistics in both graphical and table formats. This section explains how the values are derived and helps you to understand the information by breaking down the Statistics tab into the three main sections, which are Performance Overview, Scan Performance, and IP Filtering Performance.

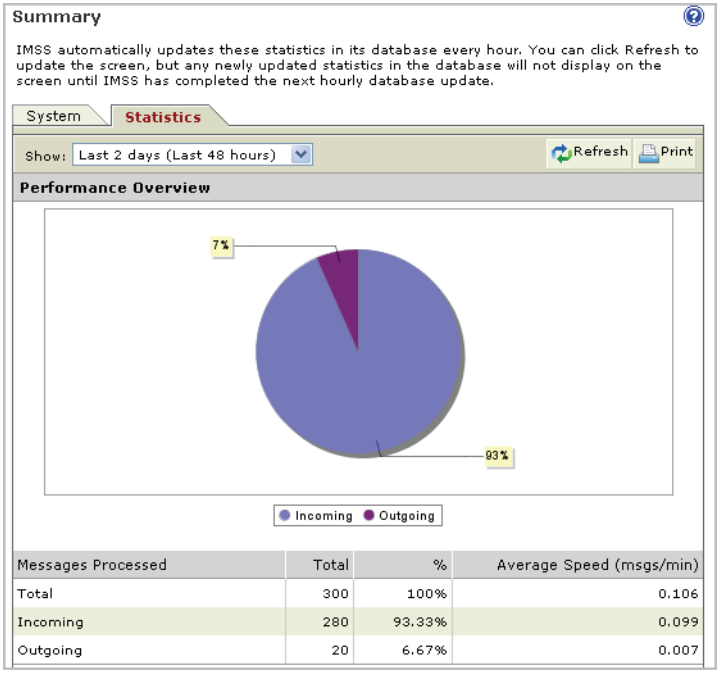
Note: 1. The values (in percentages) for the same type of threat shown in the chart and table are computed differently.

2. In the table, the total number of messages matching each scanning condition or IP filtering type consists of overlaps. For example, if a message matches more than one scanning condition, such as spam and attachment, this message will be counted twice, once in the total number for spam and a second time in the total number for attachment. Values in the chart, however, do not include such overlaps.

Performance Overview

This section shows the total number of incoming and outgoing messages in your network and their corresponding values measured as percentages of the total. The total number includes messages blocked by the following components in ascending order:

- IP Profiler
- ERS
- Scan engine



Messages Processed	Total	%	Average Speed (msgs/min)
Total	300	100%	0.106
Incoming	280	93.33%	0.099
Outgoing	20	6.67%	0.007

Scan Performance

This section shows a breakdown of the number of messages matching various types of scanning conditions specified in the policy rules, and their corresponding values in percentages.

- Chart

  Value = Number of messages matching the specific scanning condition divided by the number of messages matching all scanning conditions.

  Example:

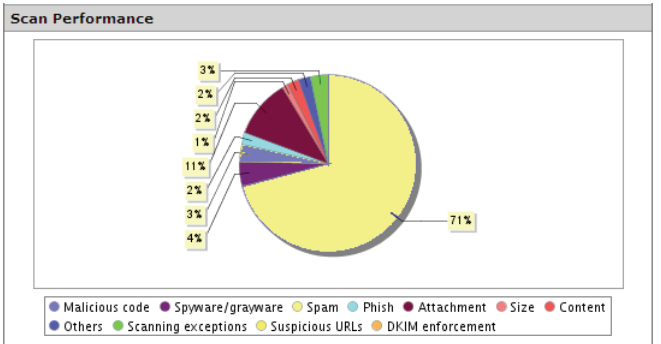
  Percentage of spam messages: 71% = 66 / 93

- Table

  Value = Number of messages matching the specific scanning condition divided by the total number of messages processed.

  Example:

Percentage of spam messages: 22% = 66 / 300



Scanning Conditions	Total	%
Malicious code	3	1%
Spyware/grayware	4	1%
Spam	66	22%
Phish	2	1%
Attachment	10	3%
Size	1	0%
Content	1	0%
Others	2	1%
Scanning exceptions	3	1%
Suspicious URLs	0	0%
DKIM enforcement	0	0%

IP Filtering Performance

This section shows the number of connections blocked by the following:

- The four types of IP Filtering rules, namely, spam, virus, DHA attack, and bounced mail
- IP addresses that you have manually entered
- ERS

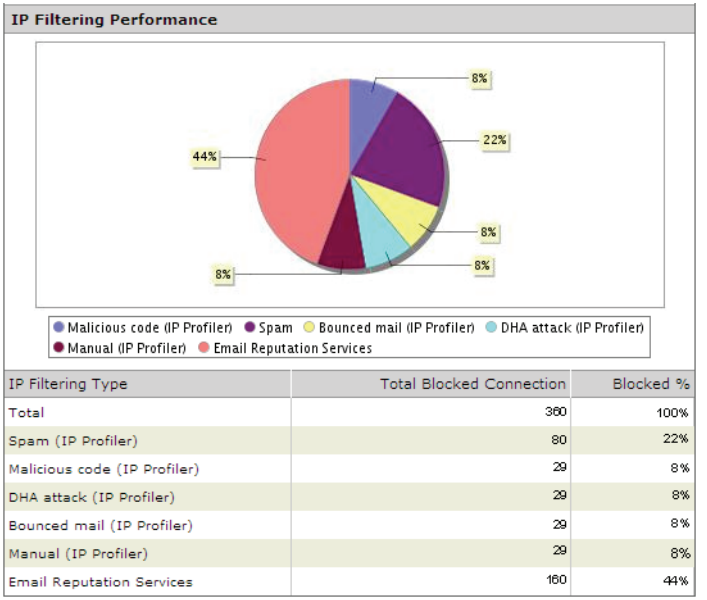
Values in the chart and table are computed as follows:

Value = Number of messages matching the specific IP filtering rule divided by the total number of messages blocked by IP Profiler and ERS.

Example:

Total number of messages blocked by IP Profiler and ERS = 360

Percentage of spam messages: 22% = 80 / 360



IP Filtering Type	Total Blocked Connection	Blocked %
Total	360	100%
Spam (IP Profiler)	80	22%
Malicious code (IP Profiler)	29	8%
DHA attack (IP Profiler)	29	8%
Bounced mail (IP Profiler)	29	8%
Manual (IP Profiler)	29	8%
Email Reputation Services	160	44%

Generating Reports

Depending on your needs, you can choose to generate a one-time report on demand or schedule a report to be run at specific intervals. IMSS offers you the flexibility of specifying the content for each report and the option of viewing or saving the result in HTML or CSV format.

Types of Report Content

You can choose from the following types of content to be included in the report:

TABLE 5-1. Report content descriptions

REPORT CONTENT	DESCRIPTIONS
Policy and traffic summary	Shows the total number and size of incoming and outgoing messages. Also shows the number of messages matching specific scanning conditions.
Virus and malicious code summary	Shows a summary of the virus message count by actions.
Spam summary	Shows a summary of the total spam message count by anti-spam engine, ERS, IP Profiler, and actions.
Sender IP address blocking summary	Includes "IP Profiler Blocking Summary" and "ERS Blocking Summary". The former shows a summary of the total number of sender connections that reached IP Profiler and are blocked by the different IP Filtering rules. The latter shows the total sender connections that reached ERS and are blocked by ERS.
Top 10 traffic email addresses	Shows the top 10 email addresses ranked by the total sent and received message count.
Top 10 virus names	Shows the top 10 virus names ranked by their detection count.
Top 10 IP addresses for DHA attack addresses	Shows the top 10 IP addresses ranked by the blocked count for DHA attack.
Top 10 IP addresses for bounced mail attack addresses	Shows the top 10 IP addresses ranked by the blocked count for bounced mail attack.
Top 10 virus recipients and senders	Shows the top 10 virus recipients and senders ranked by their total received and sent virus message counts.
Top 10 most frequently triggered rule names	Shows the top 10 rule names ranked by the number of messages that triggered each rule.

TABLE 5-1. Report content descriptions

REPORT CONTENT	DESCRIPTIONS
Top 10 spam recipients	Shows the top 10 spam recipient addresses ranked by their total received spam message count.
Top 10 IP addresses blocked by ERS	Top 10 blocked IP addresses ranked by the number of connections dropped by ERS.
Top 10 IP addresses blocked by spam	Top 10 IP addresses ranked by the blocked count for spam.
Top 10 IP addresses blocked by viruses or malicious code	Top 10 IP addresses ranked by the blocked count for viruses.
Top 10 senders of messages that contained suspicious URLs	Top 10 sender addresses ranked by their total received messages that contained suspicious URLs.

Managing One-time Reports

Generate a one-time report for an at-a-glance summary of IMSS protection. For future reference, IMSS retains all one-time reports on this screen.

You can also enable IMSS to automatically generate daily, weekly, or monthly reports.

To manage one-time reports:

1. Choose **Reports > One-time Reports** from the menu. The One-time Reports screen appears with a list of the one-time reports that you previously generated.
2. To change the display, do any of the following:
   - To sort the table, click any of the column headings that are underlined.
   - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select a number from the drop down box that represents which page to view.
   - To change the number of items that appear in the list at a time, select a new display value from the drop down box at the bottom of the table.
3. To generate a report, click **Add**. The report takes several minutes to generate. **In progress** appears in the Output column if the report is not finished generating.
4. To view the report, click one of the following formats under **Output**:

- **HTML:** Opens the report in another browser window.
- **CSV:** Saves the report as a comma separated value file that you can open with a spreadsheet application.

5. To delete a report, select the check box next to it and click **Delete**.

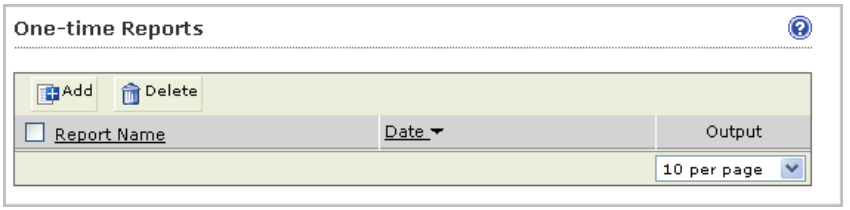
Note: ERS and IP Profiler report content is not available unless you activate those products. For more information on activating ERS and IP Profiler, see Managing Product Licenses on page 7-13.

Adding One-time Reports

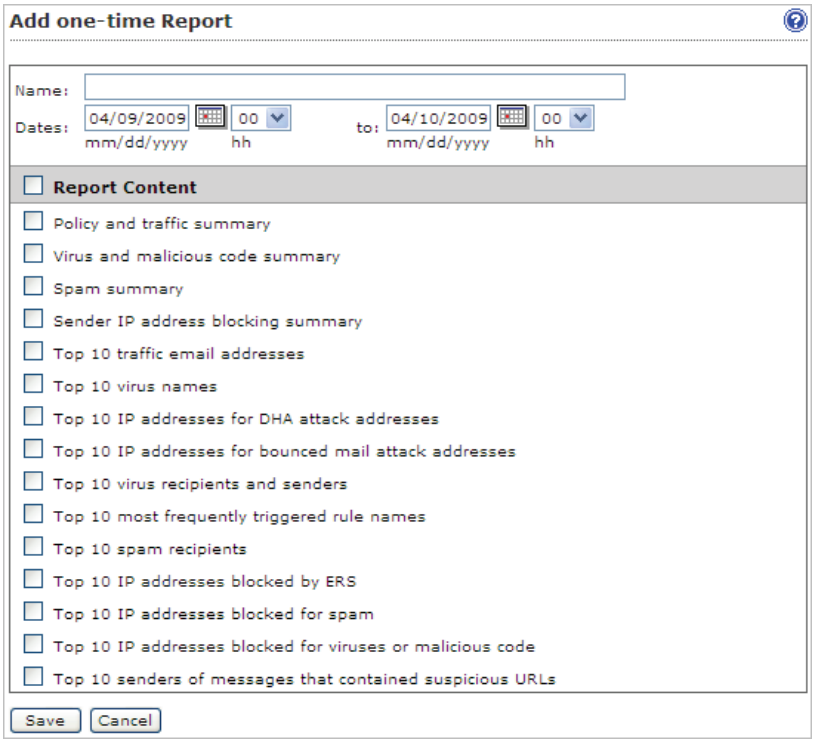
You can generate one-time reports on demand to help monitor the traffic on your network.

To create a one-time report:

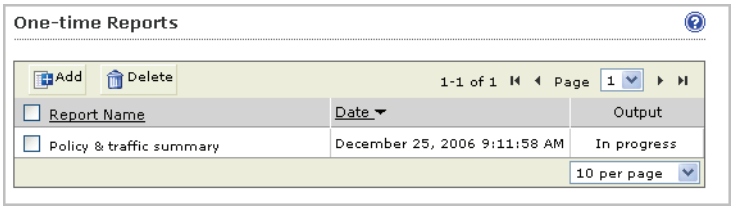
1. Choose **Reports > One-time Report** from the menu.



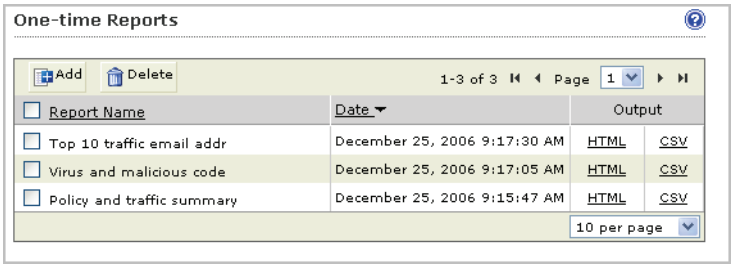
2. Click **Add**. The Add One-time Report screen appears.



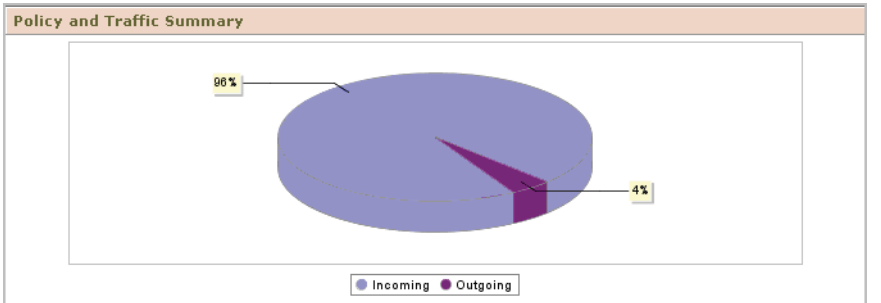
3. Next to **Name**, type a descriptive name.
4. Next to **Dates**, select the time span that the report will cover.
5. Under **Report Content**, select the content to include in the report.
6. Click **Save**. The report takes several minutes to generate. The message **In progress** appears in the report table.



After the report generates, the hyperlinks **HTML** and **CSV** display in the report table.



7. Click **HTML** to display the report in HTML format.
8. Click **CSV** to export the report data to a csv file.



Traffic Summary	Total		Incoming	Outgoing
Total # of messages	460		440	20
Total size of messages (MB)	4.558		3.374	1.184

Note: Report generation occurs once every five minutes. This means that report generation could require as much as five minutes in addition to the time required to aggregate reporting data and make the necessary calculations.

Using Scheduled Reports

Schedule reports to automate report generation. IMSS offers daily, weekly, and monthly reports.

To manage scheduled reports:

1. Click **Reports > Scheduled Reports** from the menu. The Schedule Reports screen appears with the **Daily** tab displayed.
2. Click the **Weekly** or **Monthly** tab to view the corresponding reports.
3. To view the report, click one of the following formats under **Output**:
   - **HTML:** Opens the report in another browser window.
   - **CSV:** Saves the report as a comma separated value file that you can open with a spreadsheet application.
4. To change the display, do one of the following:
   - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page.

- To change the number of items that appears in the list at a time, select a new display value from the drop-down box at the bottom of the table.

5. To delete a report, select the check box next to it and click **Delete**.

Configuring Scheduled Reports

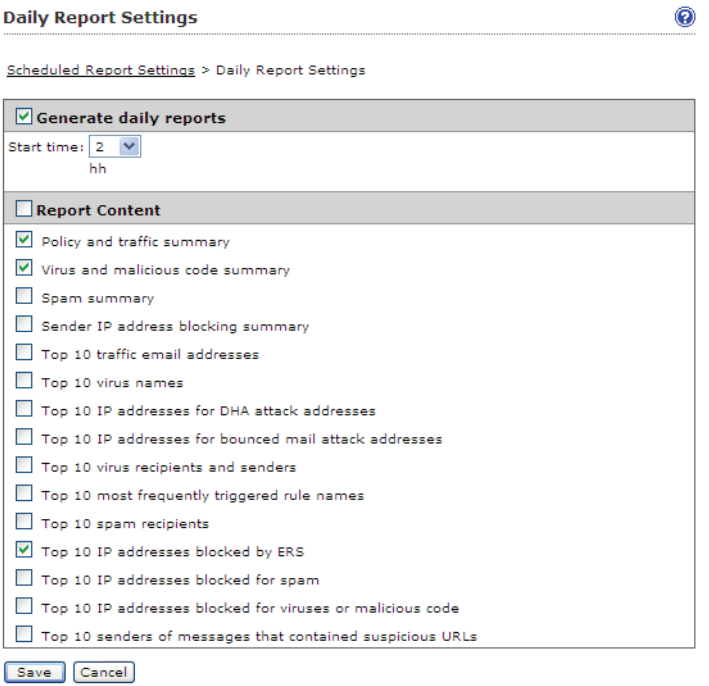
Scheduled reports generate automatically according to the intervals you configure.

To create a scheduled report:

1. Choose **Reports > Settings** from the menu. The Scheduled Report Settings screen appears.

2. Click the **Settings** link for one of the following report types:
   - Daily reports
   - Weekly reports
   - Monthly reports

   The Report Settings screen appears.



3. Specify your settings for the report.

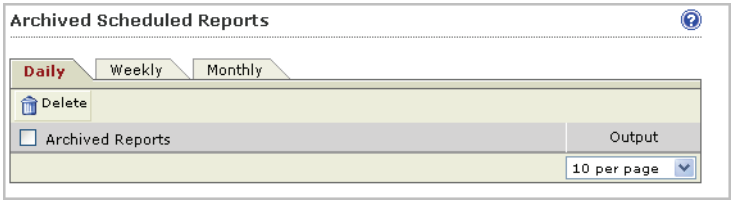
Note: When configuring monthly report settings, if you choose to generate the report on the 29th, 30th, or 31st day, IMSS will generate the report on the last day of the month for months with fewer days. For example, if you select 31, IMSS will generate the report on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

---

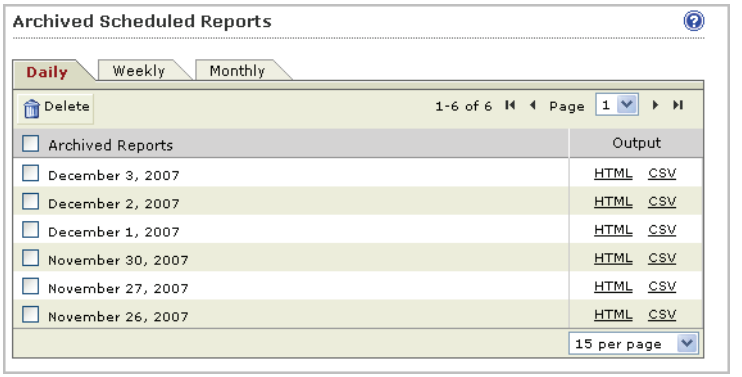
4. Click **Save**. The report status changes.

5. Specify the number for each type of report that you would like to retain. Click **Save**.
6. Choose **Reports > Scheduled Reports** from the menu. The Scheduled Reports screen appears.

Note: The report has not generated yet.



7. After the report generates, you can click **HTML** or **CSV** to view the report.



Logs

Logs are a useful means of enabling you to monitor various types of events and information flow within IMSS. They also serve as an important resource for troubleshooting.

To enable logs and benefit from the information, do the following:

Step 1. Configure the log settings

Step 2. Perform log query

Configuring Log Settings

You can configure the level of detail that IMSS writes to the logs and the length of time it stores them. In addition, you can set the update period that controls how frequently the scanner services write their local logs to the IMSS admin database.

To configure log settings:

1. Choose **Logs > Settings** from the menu.
2. Under **Reporting Logs**, configure the following:
   - **Database log update interval:** IMSS updates the logs regularly at every interval. Select a number between 1 and 60 for the interval. Selecting 60 means that IMSS updates the logs once every hour.

- **Number of days to keep logs for query:** Type a value between 1 and 60 that represents the number of days IMSS preserves the report logs in the IMSS admin database.

3. Under **Log Files**, configure the following:
   - **Application log detail level:** The level of log detail. Select one of the following:
     - **Normal:** The standard level of detail. This level provides the basic information needed by an administrator for daily monitoring and maintenance.
     - **Detailed:** A high level of detail. All IMSS processes write detailed information to the logs, including: telnet session information, the policy matched, the filter executed, and the action taken.
     - **Diagnostic:** Comprehensive information on each event or action. Diagnostic level logs include all information from the detailed level, plus SMTP routing information, and the route match information that determined which policy was applied.
     - **Debug:** The most complete and verbose level of detail. Debug logs are only recommended when troubleshooting.

Note: Diagnostic or debug logs might consume excessive IMSS resources and could lower system performance.

   - **Number of days to keep log files:** Select the check box and type a number between 1 and 150 that represents the number of days IMSS keeps the local log files. To prevent IMSS from deleting the log files, clear the check box.
   - **Maximum log file size for each service:** Select the check box and type a number between 100 and 99999 that represents the size in MB for local log files for each type of process or service. To remove any size restriction, clear the check box.

Note: IMSS log files are stored in the folder /opt/trend/imss/logs. IP Profiler log files are stored in the folder /opt/trend/ipprofiler/logs.

Daily log files for each event type are created at midnight and have the suffix "<Date>.<Count>". The <Count> suffix is incremented if there is more than one (1) log file per day.

If the log file size exceeds the maximum log file size for each service, IMSS will delete the oldest file.

4. Click **Save**.

Querying Logs

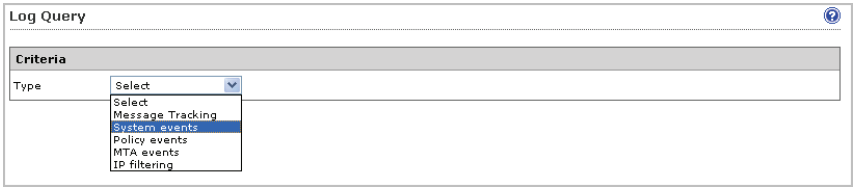
You can perform queries on five types of events or information:

- **Message tracking:** Records message details such as the sender, recipient(s), message size, and the final action that IMSS has taken. In the case of quarantined messages, the query result will also indicate the name and type of the policy rule that was triggered.
- **System events:** Tracks the time of system events such as user access, modification of rules, registration of Control Manager agent and so on.
- **Policy events:** Provides details on the policy rules that were triggered, the actions taken, and the message details.
- **MTA events:** Provides connection details of Postfix on the local computer where the central controller is installed.
- **IP Filtering:** Provides the time when IMSS started and stopped blocking email messages from the queried IP address.

For most log queries, IMSS supports wildcards (*) and exact matches (for example, to view mail recipients whose name includes A or B, set the recipient(s) to "`*A*;*B*`"). IMSS uses exact matching by default. Leaving the search condition blank displays all logs. For multiple-condition items, use semicolons (;) to separate the entries for recipient(s) and attachment(s).

To query message tracking logs:

1. Choose **Logs > Query** from the menu. The Log Query screen appears.



2. Next to **Type**, select **Message tracking**. The query screen for message event logs appears.
3. Next to **Dates**, select a date and time range.
4. Type any of the following additional information:
   - **Subject**
   - **Message ID**
   - **Sender**
   - **Recipient(s)**

Note: Use the asterisk wildcard for partial searches on any field.

---

5. Click **Display Log**. A timestamp, sender, recipient, subject, and last known action appear for each event.
6. Click the timestamp link to see the following information:
   - **Timestamp**
   - **Sender**
   - **Recipient**
   - **Subject**
   - **Message size in MB**
   - **Message ID**
   - **Scanner that detected the message**
   - **Final action that IMSS took on the message**
   - **Action details**

7. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma separated value file, click **Export to CSV**.

To query system event logs:

1. Choose **Logs > Query** from the menu.
2. Next to **Type**, select **System events**. The query screen for system event logs appears.
3. In the second drop down box next to **Type**, select one of the following:
   - **All events:** Displays the timestamp and descriptions for all system events.
   - **Updates:** Displays the timestamp of successful scan engine and pattern file updates from the ActiveUpdate server to the IMSS admin database.
   - **Service Status:** Displays the timestamp and descriptions when the scanner service is started or stopped.
   - **Admin activity:** Displays the timestamp and descriptions for major admin activities such as changing IMSS settings, admin account logons and logoffs.
   - **Errors:** Displays the timestamp and descriptions for all errors that IMSS encountered, such as unsuccessful update of the scan engine and pattern files.
4. In the third drop down box next to **Type**, select the server to view.
5. Next to **Dates**, select a date and time range.
6. Next to **Keyword in description**, type any special words to search for.
7. Click **Display Log**. A timestamp, component, and description appear for each event.
8. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop down box on the top of the table.
   - To sort the table, click the column title.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma separated value file, click **Export to CSV**.

To view policy event logs:

1. Choose **Logs > Query** from the menu.
2. Next to **Type**, select **Policy events**. The query screen for policy event logs appears.
3. In the second drop down box next to **Type**, select one of the following items related to the policy and the rules you configured for the policy:
   - **All**
   - **Virus or malicious code**
   - **Spam/phish**
   - **Web Reputation**
   - **DKIM enforcement**
   - **Attachment**
   - **Size**
   - **Content**
   - **Others**
   - **Scanning exceptions**
4. Type any of the following additional information:
   - **Senders**
   - **Recipient(s)**
   - **Rule**
   - **Subject**
   - **Attachment(s)**
   - **Message ID**

Note: If you leave any text box blank, all results for that item appear.

---

5. Click **Display Log**. A timestamp, action, rule, and message ID appear for each event.
6. Click the timestamp link to see the following information:
   - **Timestamp**
   - **Sender**
   - **Recipient**

- **Subject**
- **URL**
- **Risk Level**
- **Message size in MB**
- **Action**
- **Message ID**
- **Scanner that detected the message**

7. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop down box on the top of the table.
   - To sort the table, click the column title.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma separated value file, click **Export to CSV**.

Note: - "*A*;*B*" means a string that has A or B.

- "A*;*B" means a string that starts with A or ends with B.

- ";" represents the OR operation.

To query MTA event logs:

1. Choose **Logs > Query** from the menu.
2. Next to **Type**, select **MTA events**. The query screen for MTA event logs appears.
3. Next to **Dates**, select a date and time range.
4. Click **Display Log**. A timestamp and MTA event description appears.
5. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop down box on the top of the table.
   - To print the query results, click **Print current page**
   - To save the query result to a comma separated value file, click **Export to CSV**.

To view IP filtering logs:

1. Choose **Logs > Query** from the menu.
2. In the second drop down box next to **Type**, select one of the following items related to IP Filtering:
   - **ERS**
   - **DHA attack**
   - **Bounced mail**
   - **Virus**
   - **Spam**
   - **Manual:** Refers to the IP addresses that you have specified in the blocked list.
   - **All**
3. Next to **Dates**, select a date and time range.
4. Next to **IP**, provide any IP address or domain name to search for.
5. Click **Display Log**. Information appears for the time that IMSS both started and stopped blocking each IP address or domain.
6. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop down box on the top of the table.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma separated value file, click **Export to CSV**.

Quarantine and Archive

Quarantine and archive are among some of the actions that you can configure IMSS to take when messages match certain rules. Generally, you configure IMSS to quarantine messages that you would like to analyze before deciding whether to delete or release to the intended recipient(s). Archive, on the other hand, allows you to store messages for future reference.

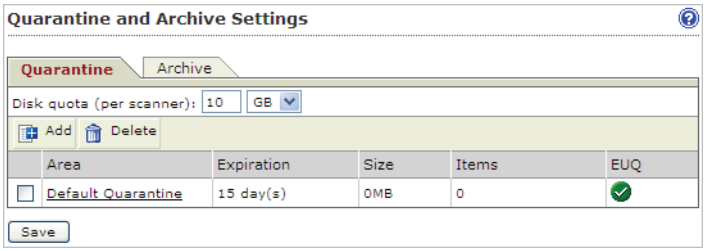
Note: In order to use End-User Quarantine, first configure the LDAP settings. For more information, see Step 3: Configuring LDAP Settings on page 1-8.

Configuring Quarantine and Archive Settings

Quarantine and archive settings allow you to manage quarantine and archive areas and allocate the amount of disk space per scanner for storing quarantined or archived messages.

To configure quarantine and archive settings:

1. Choose **Quarantine & Archive** > **Settings** from the menu. The Quarantine and Archive Settings screen appears.



2. To configure a quarantine area or an archive area, click the **Quarantine** tab (default) or **Archive** tab respectively. The list of areas appears in the table below.
3. To modify the total disk size allowed for all quarantine areas or archive areas for each scanner service, type the size of the area next to **Disk quota (per scanner)**, and then select **MB** or **GB** from the drop down box.
4. To add a quarantine or archive area, click **Add** and do the following:

5. Next to **Name**, type a descriptive name.
6. Next to **Delete messages older than**, type the number of days after which IMSS deletes the quarantined or archived messages. The value is exclusive. For example, if you type 15, IMSS deletes the quarantined messages on the 16th day.
7. Select **Synchronize all spam and email messages, that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only)**, to automatically save messages to the EUQ database.

   Note: After selecting **Synchronize all spam and email messages, that do not violate virus, phishing or Web reputation rules, to the EUQ database (for this area only**), a check mark appears under the EUQ column of the table on the Quarantine and Archive Settings screen.

8. Click **Save**. The Quarantine and Archive Settings screen reappears.
9. To view or modify a quarantine or archive area, click the name of the area and configure the settings above.
10. To delete a quarantine or archive area, select the check box next to it and click **Delete**.
11. After modifying any settings, click **Save**.

Managing Quarantine Areas

IMSS can quarantine messages on the server in the $IMSS_HOME/queue/quarantine directory.

Tip: Trend Micro recommends quarantining messages that you think you might want to analyze and possibly send to the intended recipient later. Create different types of quarantine areas for different types of email, such as email that violates spam scanning conditions or email that violates message content conditions.

You can get to a screen to modify quarantine areas from one of the following screens:

From the Actions screen of a policy rule:

If you are configuring the actions for a rule, do the following:

1. Click **Edit** next to **Quarantine to** under **Intercept** actions. The Quarantines screen appears showing the available quarantine areas.
2. To add a new quarantine area, click **Add**. To modify an existing quarantine area, click the area name and then click **Edit**. An edit screen appears.
3. Next to **Name**, type the name of the quarantine area.
4. To automatically delete quarantined email after a certain number of days, next to **Delete messages older than**, type the number of days from 1 to 60. This number represents the number of days after which IMSS deletes the quarantined messages. The value is exclusive. For example, if you type 15, IMSS deletes the quarantined messages on the 16th day.
5. Select **Synchronize all spam and email messages, that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only)**, to automatically save messages to the EUQ database.

Note: After selecting **Synchronize all spam and email messages, that do not violate virus, phishing or Web reputation rules, to the EUQ database (for this area only)**, a check mark appears under the EUQ column of the table on the Quarantine and Archive Settings screen.

---

6. Click **Save** to return to the Quarantines screen.
7. Click **Done** to continue selecting actions.
8. To quarantine messages, select the radio button next to **Quarantine to** under **Intercept** and select the desired quarantine area from the drop down box.

From Quarantine & Archive > Settings:

1. Click **Quarantine & Archive > Settings**. The Quarantine and Archive Settings screen appears with the **Quarantine** tab displayed by default.
2. Next to **Disk quota per scanner service**, do the following:
   a. Type the maximum size for the area.
   b. Select **MB** or **GB**.

Note: When the total disk size for all the quarantined email messages exceeds the quota on a scanner, the oldest quarantined messages are deleted first to keep the size under the quota.

---

3. To add a new quarantine area, click **Add**. To modify an existing quarantine area, click the area name. An edit screen appears.
4. Next to **Name**, type the name of the quarantine area.
5. To automatically delete quarantined email after a certain number of days, next to **Delete messages older than**, type the number of days from 1 to 60. This number represents the number of days after which IMSS deletes the quarantined messages. The value is exclusive. For example, if you type 15, IMSS deletes the quarantined messages on the 16th day.
6. Select **Synchronize all spam and email messages, that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only)**, to automatically save messages to the EUQ database.

Note: After selecting **Synchronize all spam and email messages, that do not violate virus, phishing or Web reputation rules, to the EUQ database (for this area only)**, a check mark appears under the EUQ column of the table on the Quarantine and Archive Settings screen.

---

7. Click **Save** to return to the Quarantine and Archive Settings screen.
8. Click **Save**.

Querying Messages

You can perform a query on quarantined and archived messages before deciding which action to perform. After viewing the message details, you can choose to release or delete the quarantined messages, or delete archived messages from IMSS.

Tip: Trend Micro recommends quarantining items that could pose a risk to your network, such as messages and attachments that violate antivirus rules. Before you resend any quarantined message, make sure that it does not pose a threat to your network.

Trend Micro recommends archiving only items that you want to reference later. Quarantine items that could pose a threat to your network, such as email messages and attachments that violated an antivirus rule.

To query quarantine areas:

1. Choose **Quarantine & Archive > Query** from the menu. The Quarantine and Archive Query screen appears. The **Quarantine** tab displays by default. If it does not display, click **Quarantine**.
2. Under **Criteria**, configure the following:
   - **Search:** Select the quarantine area, the reason the email was quarantined, and the scanner that scanned the email.
   - **Dates:** Select a date and time range.
3. Type values for the following:
   - **Sender**
   - **Subject**
   - **Recipient**
   - **Attachment**
   - **Rule**
   - **Message ID**

Note: When querying an email containing multiple recipients or attachments, type *string* (where string is the name of one of the recipients or attachments).

4. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, subject, and reason for quarantining the message.
5. To change the display, do any of the following:
   - To sort the table, click any of the column headings (except reason).
   - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select the desired page to view from the drop-down list.
   - To change the number of items that appears in the list at a time, select a new display value from the drop-down list at the bottom of the table.
6. To view details about any quarantined message, click the timestamp for the item. The Quarantine Query screen appears showing the email message and all of its details.
7. To resend any message, click the check box next to it in the query result table, and then click **Deliver** or **Reprocess**.

   Deliver: The message is sent directly to the recipient, by passing all rules except virus scan rules.

   Reprocess: The message only bypasses the current rule, and may be quarantined again by other filters.

   Tip: Trend Micro does not recommend resending email messages that violated antivirus filters. Doing so could put your network at risk.

8. To delete any message, click the check box next to it in the query result table, and then click **Delete**.

   Note: IMSS only records and shows names of attachments if you have specified Attachment as a scanning condition. However, if the number of attachments in the email exceeds the maximum number specified in the condition, the attachment name will not be shown.

To query archive areas:

1. Choose **Mail Areas & Queues > Query** from the menu. The **Quarantine** tab displays by default.
2. Click the **Archive** tab.

3. Under **Criteria**, configure the following:
   - **Search:** Select the archive area, the reason the email was archived, and the scanner that scans the email.
   - **Dates:** Select a time range.
4. Type values for the following:
   - **Sender**
   - **Subject**
   - **Recipient**
   - **Attachment**
   - **Rule**
   - **Message ID**

Note: When querying an email containing multiple recipients or attachments, type *string* (where string is the name of one of the recipients or attachments).

---

5. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, subject, and reason for archiving the message.
6. To change the display, do any of the following:
   - To sort the table, click any of the column headings (except reason).
   - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select the desired page to view from the drop-down list.
   - To change the number of items that appears in the list at a time, select a new display value from the drop-down list at the bottom of the table.
7. To view details about any archived message, click the timestamp for the item. The Archive Query screen appears showing the email message and all of its details.

8. To delete any message, click the check box next to it in the query result table, and then click **Delete**.

Note: IMSS only records and shows names of attachments if you have specified Attachment as a scanning condition. However, if the number of attachments in the email exceeds the maximum number specified in the condition, the attachment name will not be shown.

Viewing a Quarantined Message

To view a quarantined message:

1. After you perform a query for quarantined messages, click the timestamp for the quarantined item in the query result table. The Quarantine Query screen appears showing the following information:
   - **Timestamp**
   - **Message ID**
   - **Sender**
   - **Reason**
   - **Recipient**
   - **Rules**
   - **Subject**
   - **Scanner**
   - **Size**
   - **Internal ID**
   - **Attachments**
2. Next to **Message view**, click either **Header** or **Message**.

3. Click any of the following buttons:
   - **Back to List:** Return to the query screen.
   - **Deliver:** Resend the message to its original recipients.
   - **Reprocess:** IMSS scans the message again and acts accordingly.
   - **Delete:** Delete the message.
   - **Download:** Save the message to your computer.

Tip: Trend Micro does not recommend saving messages or attachments that violated an antivirus rule.

Viewing Archived Messages

To view archived messages:

1. After you perform a query for archived messages, click the timestamp for the quarantined item in the query result table. The Archive Query screen appears showing the following information:
   - **Timestamp**
   - **Message ID**
   - **Sender**
   - **Reason**
   - **Recipient**
   - **Rules**
   - **Subject**
   - **Scanner**
   - **Size**
   - **Internal ID**
   - **Attachments**
2. Next to **Message view**, click either **Header** or **Message**.

3. Click any of the following buttons:
   - **Back to List:** Return to the query screen.
   - **Delete:** Delete the message.
   - **Download:** Save the message to your computer.

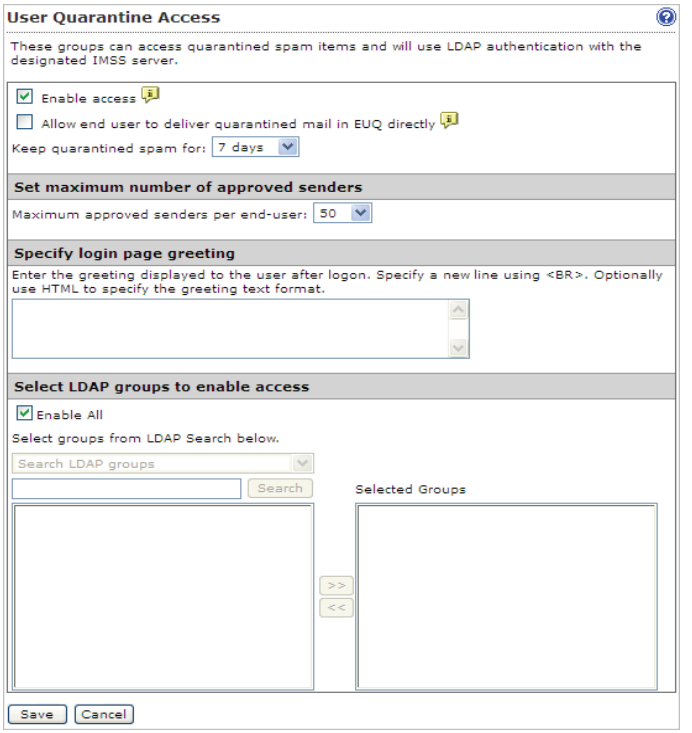
Tip: Trend Micro does not recommend saving messages or attachments that violated an antivirus rule.

Configuring User Quarantine Access

You can grant all or selected end-users access to the EUQ Web console so that they can manage the spam messages addressed to them by visiting `https://<target server IP address>:8447`.

To configure user quarantine access:

1. Click **Administration** > **User Quarantine Access**. The User Quarantine Access screen appears.



2. Select **Enable access**.
3. Select **Allow end user to deliver quarantined mail in EUQ directly** to allow end users to deliver quarantined messages directly to the recipient. The message bypasses all rules except virus scanning rules.
4. Select the number of days to keep quarantined spam.
5. Select the maximum number of senders each end-user can approve when sifting through the quarantined email messages.
6. Type a log on page message that appears on the user's browser when he/she starts to access the quarantined email messages.

7. Under **Select LDAP groups**, select the check box next to **Enable all** to allow all LDAP group users to access quarantined spam.
8. To add individual LDAP groups, clear the **Enable all** check box and do either of the following:

   Search for groups:

   a. From the drop down list, select Search LDAP groups.

   b. Type the group name.

   c. Click **Search**. The groups appear in the table below.

   d. Click the LDAP groups to add.

   e. Click **>>**. The groups appear in the **Selected Groups** table.

   Browse existing groups:

   a. From the drop down list, select **Browse LDAP groups**. The groups appear in the table below.

   b. Click the LDAP groups to add.

   c. Click **>>**. The groups appear in the **Selected Groups** table.
9. Click **Save**.

Note: When enabling user quarantine access for an LDAP group, you can use wildcards in the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server. For example, A*, *A, *A* are all allowed. If you have selected Domino as the LDAP server, you can only use wildcards at the end. For example, *A, *A* are not allowed.

Adding an EUQ Database

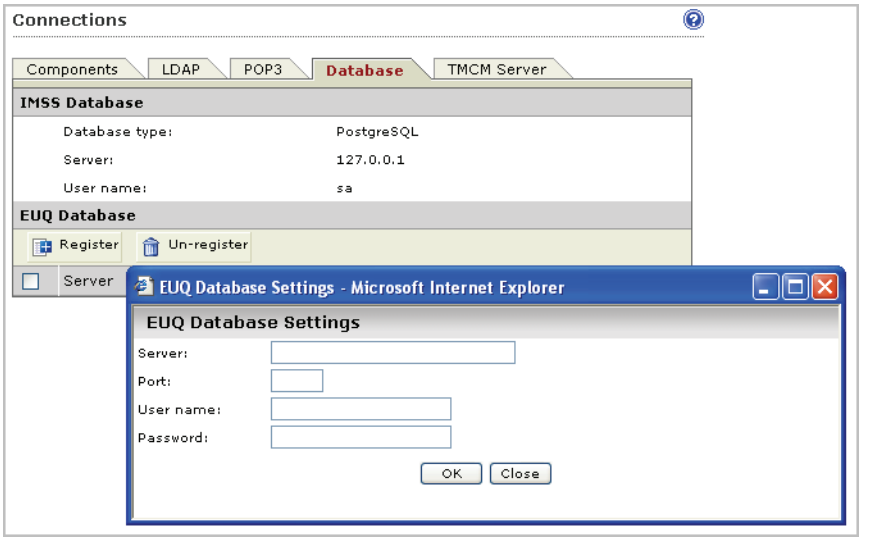
If you have an existing EUQ database, you may add new EUQ databases if you want to do the following:

- Perform load balancing
- Allow more end-users to access EUQ

You may register an EUQ database from the Web management console if the database was already installed but unregistered. Otherwise, run the IMSS installation program to add a new EUQ database to the system.

To register an EUQ database:

1. Choose **Administration** > **IMSS Configuration** > **Connections** from the menu. The Components tab appears by default.
2. Click the **Database** tab.
3. Click the **Register** button. The EUQ Database Settings screen appears.



4. Provide the required information.
5. Click **OK**.

Command-line options for euqtrans tool

The command-line options for the euqtrans script are as follows:

all: Transfer the individual Approved Senders Lists and information about the quarantined mail messages from the database that was removed to the new location (database) based on the updated Table and Database mapping.

approvedsender: Transfer the individual Approved Senders Lists from the database that was removed to the new location (database) based on the new mapping.

Event Notifications

You can configure IMSS to send an email or SNMP notification to you or specific email users upon the occurrence of the following categories of event:

- **System Status:** Informs you when certain IMSS performances fall below the desired level. For example, when a scanner service stops working, or when the number of messages in the delivery queue exceeds the desired quantity.
- **Scheduled Update Event:** Alerts you when IMSS is able or unable to perform a scheduled update of the scan engine or pattern files from the update source onto the admin database.
- **Scanner Update Result:** Alerts you when IMSS is unable to update the engine or pattern files on any scanner.

Note: Component update is a 2-step process:
1. At the scheduled time, the IMSS admin database will first check the update source for new engine or pattern files.

2. IMSS scanners will then check the admin database at regular intervals for updated components. The default interval is three minutes.

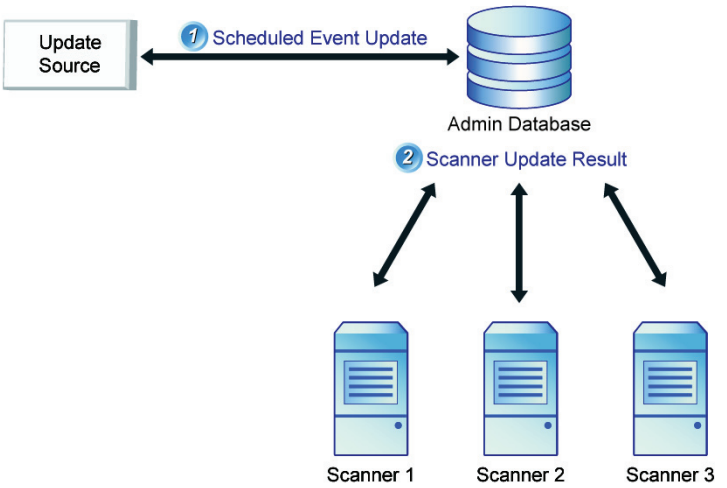


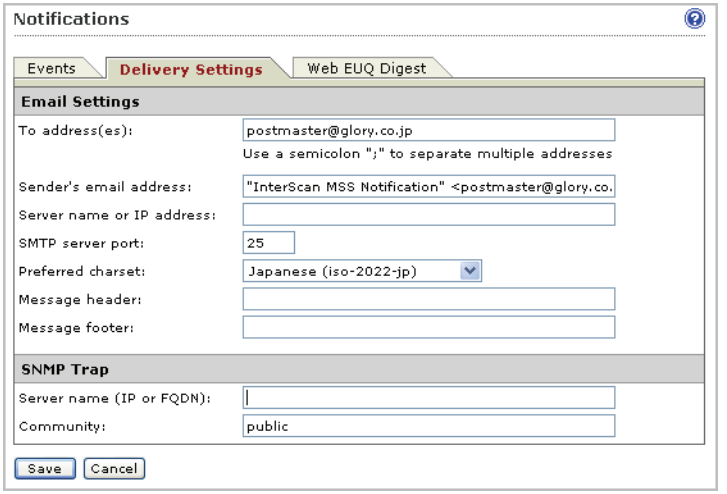
FIGURE 5-1. Scan engine and pattern file updates

Configuring Delivery Settings

The delivery settings allow you to specify the sender, recipient(s) and other settings required for delivering the notification message when certain events are triggered.

To configure the delivery settings:

1. Choose **Administration** > **Notifications** from the menu. The Events tab appears by default.
2. Click the **Delivery Settings** tab.



3. Under **Email Settings**, configure the following:
   - **To address(es):** Type the recipient email addresses.
   - **Sender's email address:** Type the email address to appear as the sender.
   - **Server name or IP address:** Type the Fully Qualified Domain Name (FQDN) or IP address of the SMTP server that delivers email on your network.
   - **SMTP server port:** Type the port number that IMSS uses to connect to the SMTP Server.
   - **Preferred charset:** IMSS will use this setting to encode the notification messages.
   - **Message header:** Type the text to appear at the top of the notification.
   - **Message footer:** Type the text to appear at the bottom of the notification.
4. Under **SNMP Trap**, configure the following:

Note: **SNMP Trap** is the notification message sent to the Simple Network Management Protocol (SNMP) server when events that require administrative attention occur.

- **Server name:** Type the FQDN or IP address of the SNMP server.
- **Community:** Type the SNMP server community name.

Note: **Community** is the group that computers and management stations running SNMP belong to. To send the alert message to all SNMP management stations, type 'public' as the community name. For more information, refer to the SNMP documentation.

5. Click **Save**.

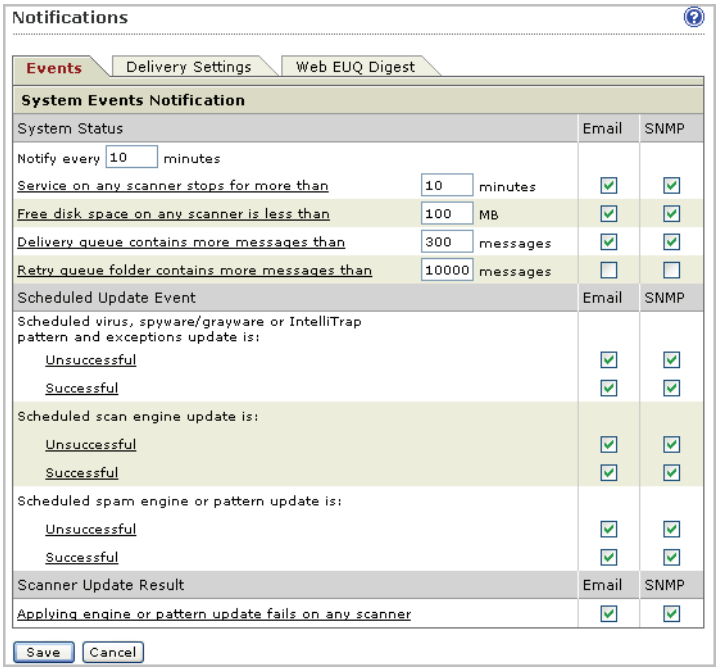
   If you are using the Configuration Wizard, click **Next**.

Configuring Event Criteria and Notification Message

You can set the criteria under which IMSS will trigger a notification message and also customize the message content for each event.

To configure the criteria and message content:

1. Choose **Administration** > **Notifications** from the menu. The Events tab appears by default.



2. Under System Status, configure the following:
   - **Notify every { } minutes:** Type the notification frequency for all performance notifications.

   To edit each of the following notifications, click the link.
   - **Service on any scanner stops for more than:** Type the number of minutes.
   - **Free disk space on any scanner is less than:** Type the number of MB.
   - **Delivery queue contains more than:** Type the number of messages.
   - **Retry queue folder contains more than:** Type the number of messages.

Note: The notifications **Delivery queue contains more than** and **Retry queue folder contains more than** only function when IMSS runs with Postfix.

3. Under **Scheduled Update Event**, click the **Unsuccessful** and **Successful** links to edit notifications for component updates.

Note: **Scheduled Update Event** is the event in which the latest engine and pattern files from the Update Source are updated onto the IMSS admin database.

4. Under **Scanner Update Results**, click the **Applying engine or pattern update fails on any scanner** link to edit the notification.

Note: **Scanner Update Results** are the results of updating the latest engine and pattern files from the IMSS admin database onto the scanners.

5. Select the **Email** and/or **SNMP** check boxes according to how you would like to receive the notification.
6. Click **Save**.

Configuring Web EUQ Digest Settings

The EUQ digest is a notification that IMSS sends to users telling them how many of their email messages are in the End-User Quarantine.

To configure Web EUQ Digest settings:

1. Choose **Administration > Notifications** from the menu. The Events tab displays by default.
2. Click **Web EUQ Digest**.
3. Select the check box next to **Enable EUQ Digest**.
4. Under **Digest Schedule**, click the radio button next to one of the following frequencies:
   - **Daily:** Select the time of day from the drop down boxes.
   - **Weekly:** Select the day and time of day from the drop down boxes.

5. Under **Digest Mail Template**, type the subject and notification content.
   To see a list of variables to include in the notification, click **Variables List**.
6. Click **Save**.

Editing Notifications

To edit notifications:

1. Choose **Administration > Notifications** from the menu.
2. Click the notification to edit. The edit screen for that notification appears.
3. Type the email subject and message, or SNMP message.
   To see a list of variables to include in the notification, click **Variables List**.
4. Click **Save**.

Chapter 6

Using End User Quarantine

This chapter explains how to use End-User Quarantine (EUQ).

Topics include:

About EUQ

IMSS provides Web-based EUQ to improve spam management. The Web-based EUQ service allows end-users to manage their own spam quarantine. Messages that are determined to be spam are quarantined. These messages are indexed into a database by the EUQ agent and are then available for end-users to review, delete, or approve for delivery.

To use EUQ, you must do the following:

Step 1: Configuring and Enabling LDAP on page 6-2

Step 2: Enabling EUQ on page 6-5

Step 3: Starting the EUQ Service on page 6-6

Step 4: Enabling End-User Access on page 6-6

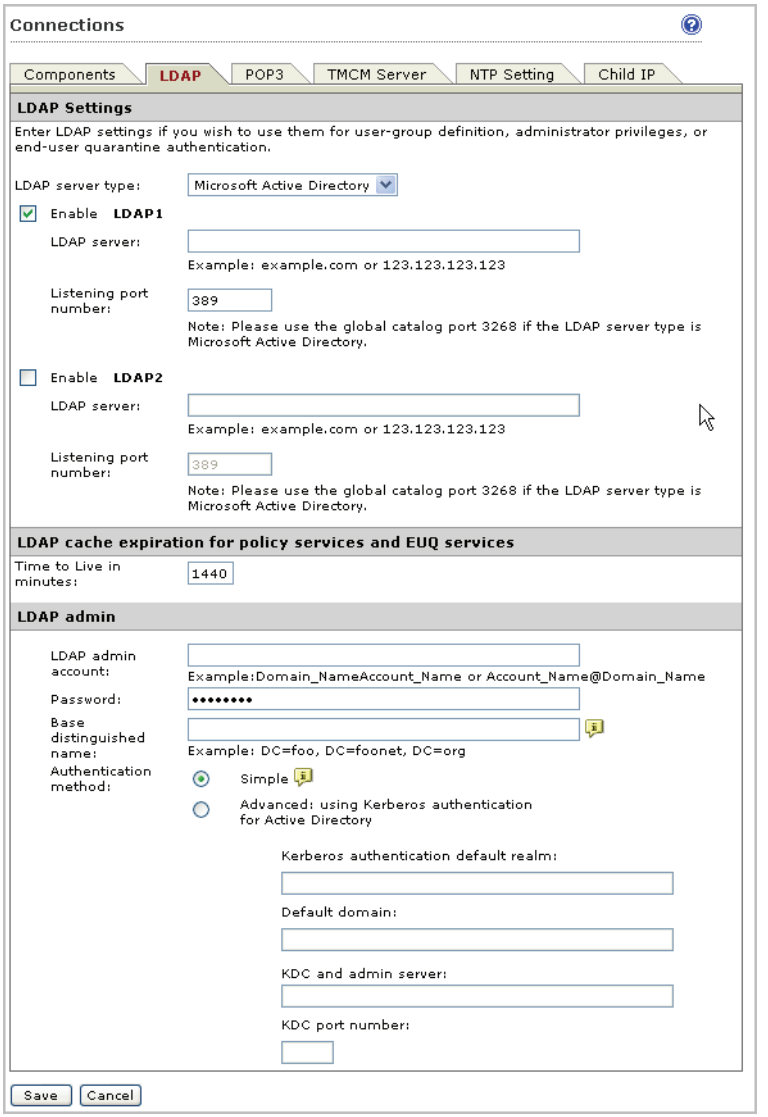
Step 5: Opening the End-User Quarantine Console on page 6-9

Step 1: Configuring and Enabling LDAP

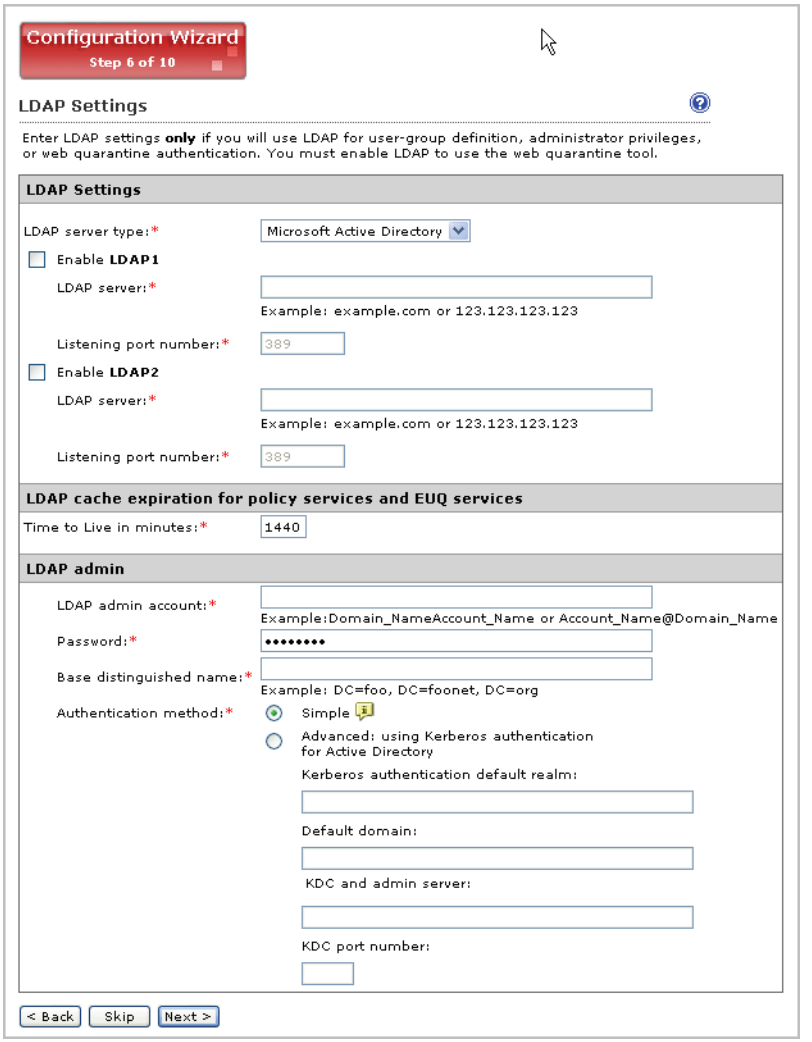
To use EUQ, you must configure and enable LDAP.

To enable and configure LDAP:

1. You can configure and enable LDAP settings in the following ways:
   - Choose **Administration > IMSS Configuration > Connections** from the menu, then click the **LDAP** tab.



- Choose **Administration > IMSS Configuration > Configuration Wizard** from the menu.

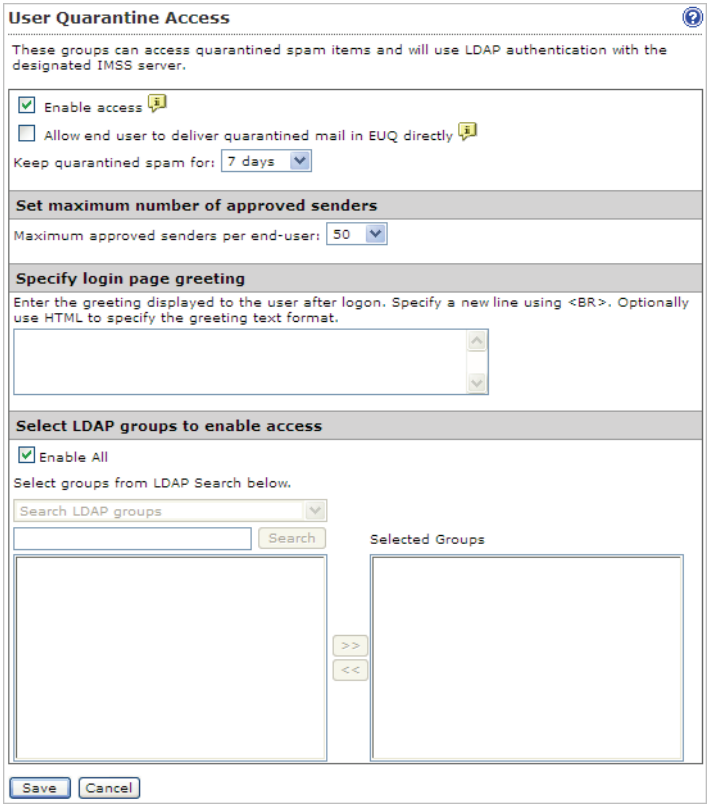


2. Configure all LDAP settings.

Step 2: Enabling EUQ

To enable EUQ:

1. Choose **Administration > User Quarantine Access** from the menu.

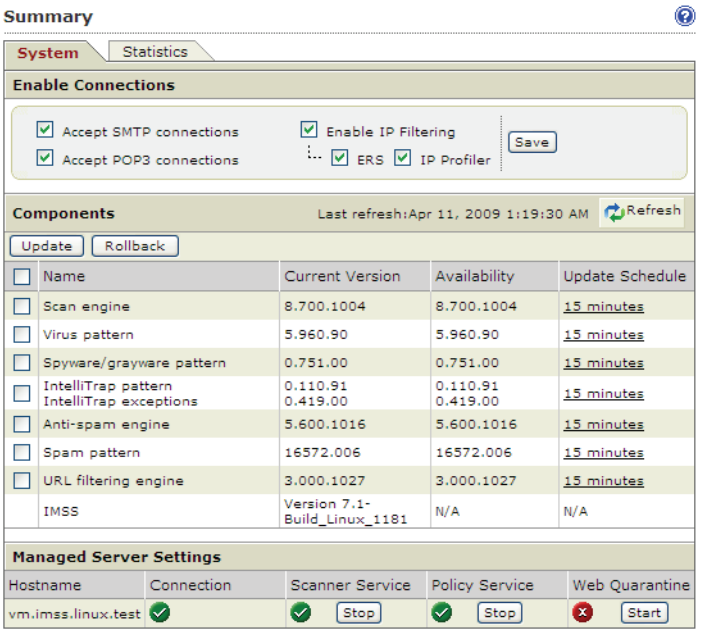


2. Select the **Enable access** check box.
3. Click **Save**.

Step 3: Starting the EUQ Service

To start the EUQ service:

1. Choose **Summary** from the menu. The System screen appears.
2. In the **Managed Server Settings** table, click **Start** under **Web Quarantine**.

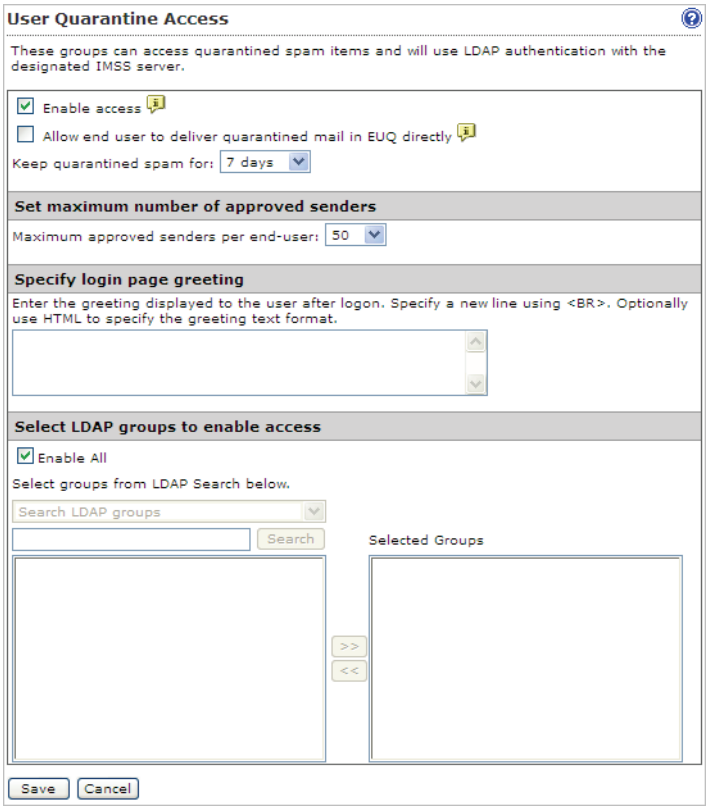


Step 4: Enabling End-User Access

Enable end-user access to allow the users to access quarantined spam items that IMSS might have misidentified as spam. The clients use LDAP authentication to access the IMSS EUQ service.

To configure and enable end-user access:

1. Choose **Administration > User Quarantine Access** from the menu. The User Quarantine Access screen appears.



2. Select **Enable access**.
3. Select **Allow end user to deliver quarantined mail in EUQ directly** to allow end users to deliver quarantined messages directly to the recipient. The message bypasses all rules except virus scanning rules.
4. Select the number of days to keep quarantined spam.
5. Select the maximum number of approved senders for each end-user.

6. Type a log on page message that appears on the user's browser when he/she starts to access the quarantined email messages.
7. Under Select LDAP groups, select the check box next to **Enable all** to allow all LDAP group users to access quarantined spam.
8. To add individual LDAP groups, clear the **Enable all** check box and do either of the following:

   Search for groups:

   a. From the drop-down list, select **Search LDAP groups**.

   b. Type the group name.

   c. Click **Search**. The groups appear in the table below.

   d. Click the LDAP groups to add.

   e. Click **>>**. The groups appear in the Selected Groups table.

   Browse existing groups:

   a. From the drop-down list, select **Browse LDAP groups**. The groups appear in the table below.

   b. Click the LDAP groups to add.

   c. Click **>>**. The groups appear in the Selected Groups table.

   d. Click **Save**.

Step 5: Opening the End-User Quarantine Console

You can view the EUQ Web console from the computer where the program was deployed or remotely across the network.

To view the console from another computer on the network, type the following URLs:

- Primary EUQ service: `https://<target server IP address>:8447`
- Secondary EUQ service: `https://<target server IP address>:8446`

WARNING! **To successfully access all Web consoles on secondary EUQ services, you must synchronize the system time of all EUQ services on your network.**

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

Logon Name Format

The format of the user logon name for accessing the EUQ Web console differs according to the LDAP server type you have selected when configuring LDAP settings. Following are some examples of the logon name format for the three types of supported LDAP servers:

- **Microsoft Active Directory**
  - Without Kerberos: `user1@domain.com (UPN) or domain\user1`
  - With Kerberos: `user1@domain.com`
- **Domino:** `user1/domain`
- **Sun iPlanet Directory:** `uid=user1, ou=people, dc=domain, dc=com`

Disabling EUQ

Before disabling EUQ, inform your users that they should handle their quarantined spam.

To disable EUQ:

1. To access the EUQ configuration screen, do one of the following:
   - Choose **Administration > User Quarantine Access** from the menu. The EUQ Management tab appears.
   - Choose **Administration > IMSS Configuration > Configuration Wizard** from the menu, then go to **Step 2: Deployment Settings**.
2. Clear the **Enable access** check box.
3. You have the option of removing all EUQ data to save disk space. To do so, click **Remove** on the EUQ Management tab.
4. Click **Save** at the EUQ Management tab. If you are using the wizard, progress through the wizard screens and click **Finish**.

Chapter 7

Performing Administrative Tasks

This chapter explains how to perform important administrative tasks, such as managing accounts, changing a device IP address, and using the backup data port.

Topics include:

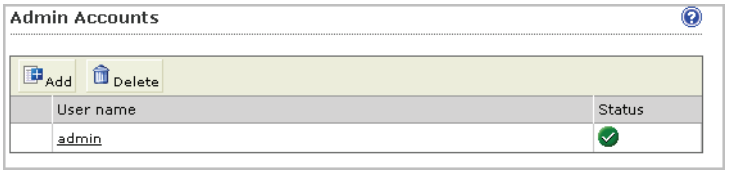
Managing Administrator Accounts

To reduce bottlenecks in administering IMSS, you can delegate administrative tasks to other staff by creating new administrator accounts and assigning the desired permissions to the various areas of the Web management console.

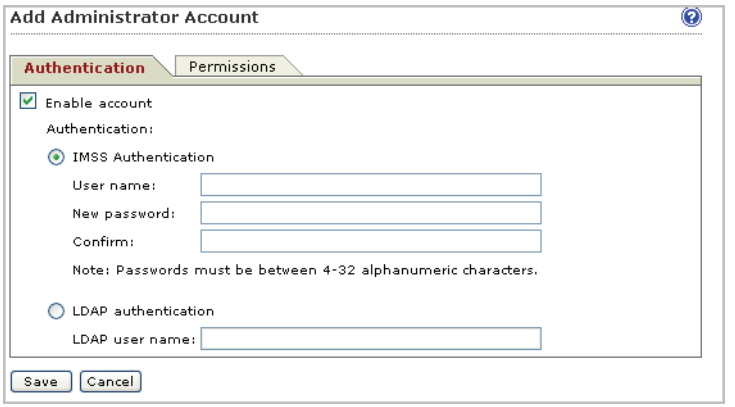
Adding Administrator Accounts

To add administrator accounts:

1. Choose **Administration** > **Admin Accounts** from the menu. The Admin Accounts screen appears.



2. Click **Add**. The Add Administrator Account screen appears with the **Authentication** tab displaying.



3. Specify Authentication settings:
   a. Select **Enable account**.

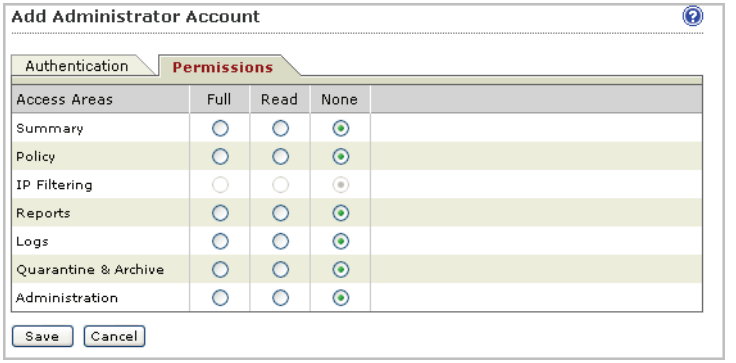
b. Select an authentication type:

- **IMSS Authentication:** Type the username, new password, and the new password confirmation.

  The password must be between 4 and 32 alphanumeric characters.
- **LDAP authentication:** Type the LDAP username.

c. Click **Save**.

4. Click the **Permissions** tab. The Permissions screen appears.



5. Specify Permissions settings:

a. Select **Full**, **Read**, or **None** for each of the following access areas that appear on the IMSS Web management console menu:

- **Summary**
- **Policy**
- **IP Filtering**
- **Reports**
- **Logs**
- **Quarantine & Archive**
- **Administration**

b. Click **Save**.

Note: 1. Only the default IMSS administrator account can add new administrator accounts. Custom administrator accounts cannot do so even if you assign full permission to the Administration area.

2. Custom administrator accounts with full administration rights can only change their own IMSS passwords. If you forget the default administrator account password, contact Trend Micro's technical support to reset the password.

Editing or Deleting Administrator Accounts

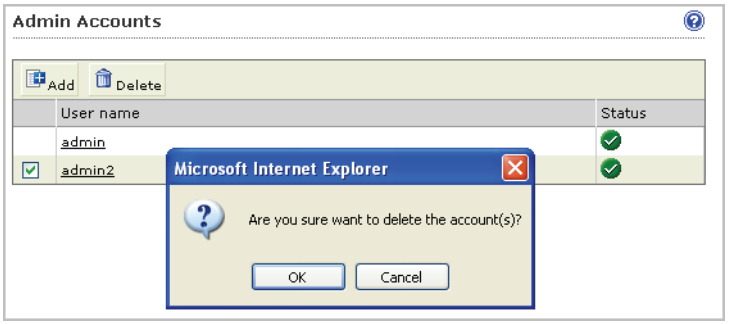
You can change or delete the permissions of a custom administrator account whenever there is a revision of roles or other organizational changes.

To edit an administrator account:

1. Choose **Administration** > **Admin Accounts** from the menu. The Admin Accounts screen appears.
2. Click the account name hyperlink.
3. Make the required changes.
4. Click **Save**.

To delete an administrator account:

1. Select the check box next to the account to be removed.
2. Click **Delete**.
3. Click **OK** to confirm the deletion.



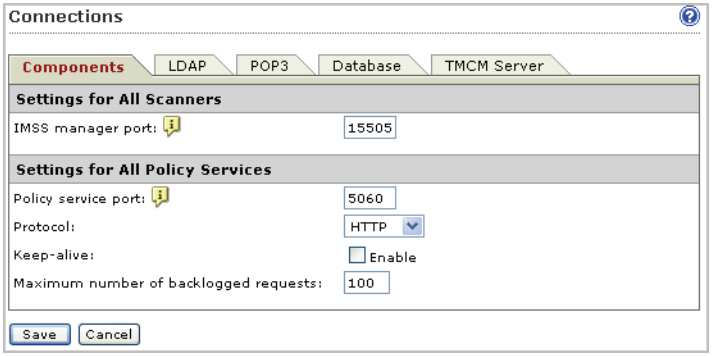
Note: You can only delete custom administrator accounts, not the default IMSS administrator account.

Configuring Connection Settings

To enable the scanner to receive messages and enhance the performance of rule lookups by the policy services, configure the connection settings.

To configure scanner and policy connections:

1. Choose **Administration** > **IMSS Configuration** > **Connections** from the menu. The Components tab appears by default.



2. Under **Settings for All Scanners**, type the port number that IMSS uses to communicate with scanners.

Note: If the user does not set the port number or the firewall could not open this port, the managed server appears as disconnected in the Summary page. Furthermore, any changes will not take effect on the managed service(s).

---

3. Under **Settings for All Policy Services**, configure the following:
   - **Policy service port:** Type the port number that IMSS uses to communicate with policy services. The default port number that the policy service uses to communicate with IMSS is 5060.
   - **Protocol:** Select the type of protocol the scanner uses to communicate with the policy service (HTTP or HTTPS).
   - **Keep-alive:** Select the check box to enhance policy retrieval by maintaining a constantly active connection between the scanner and policy services.

- **Maximum number of backlogged requests:** Type a number that represents the maximum number of requests IMSS will preserve until it can process them later.

4. Click **Save**.

Configuring LDAP Settings

Configure LDAP settings for user-group definition, administrator privileges, or end-user quarantine authentication. You can enable up to two LDAP servers for each IMSS group.

To provide a backup LDAP server, configure two LDAP servers.

To configure LDAP settings:

1. Choose **Administration > IMSS Configuration > Connections**. The **Components** tab displays by default.
2. Click the **LDAP** tab.
3. Next to **LDAP server type**, choose the type of LDAP servers on your network:
   - **Microsoft Active Directory**
   - **Domino**
   - **Sun iPlanet Directory**
4. Next to **Enable LDAP 1**, select the check box.
5. Next to **LDAP server**, type the server name or IP address.
6. Next to **Listening port number**, type the port number that the LDAP server uses to listen to access requests.
7. Configure the settings under **LDAP 2** if necessary.
8. Under **LDAP cache expiration for policy services and EUQ services**, type the **Time to live** in minutes.

   Time To Live: Determines how long IMSS retains the LDAP query results in the cache. Specifying a longer duration enhances LDAP query during policy execution. However, the policy server will be less responsive to changes in the LDAP server. A shorter duration means that IMSS has to perform the LDAP query more often, thus lowering the performance.

9. Under **LDAP admin**, type the administrator account, the corresponding password and the base distinguished name. Refer to the table below for assistance on what to specify under this section according to the LDAP server type:

TABLE 7-1. LDAP Server Types

LDAP SERVER	LDAP ADMIN ACCOUNT (EXAMPLES)	BASE DISTINGUISHED NAME (EXAMPLES)	AUTHENTICATION METHOD
Active Directory	Without Kerberos: user1@domain.com (UPN) or domain\user1 With Kerberos: user1@domain.com	dc=domain, dc=com	Simple Advanced (with Kerberos)
Domino	user1/domain	Not applicable	Simple
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	Simple

10. Select an authentication method:
    - **Simple**
    - **Advanced:** Uses Kerberos authentication for Active Directory. Configure the following:
        - **Kerberos authentication default realm:** Default Kerberos realm for the client. For Active Directory it must be the Windows domain name in upper case (Kerberos is case-sensitive).
        - **Default domain:** The Internet domain name equivalent to the realm.
        - **KDC and admin server:** Hostname or IP address of the Key Distribution Center for this realm. For Active Directory, it is usually the domain controller.
        - **KDC port number:** The associated port number.
11. Click **Save**.

    If you are using the Configuration Wizard, click **Next**.

Note: IBM Domino and Sun iPlanet only support Simple Authentication method.

If the domain name in LDAP administrator account can be resolved by DNS, the Kerberos authentication will succeed no matter what value you type in the default realm.
If the domain name in LDAP administrator account cannot be resolved, Kerberos will use the default realm to check.

Configuring POP3 Settings

In addition to SMTP traffic, IMSS can scan POP3 messages at the gateway as your clients retrieve them.

Tip: To use the POP3 message filter, enable **Accept POP3 connection** from **Summary > System** screen. This option is not selected by default.

To configure POP3 settings:

1. Choose **Administration > IMSS Configuration > Connections**. The **Components** tab displays by default.
2. Click the **POP3** tab.
3. To configure a connection from unknown POP3 servers on the Internet, type the port number IMSS uses for incoming POP3 connections under **Generic POP3 Connection**.
4. To configure connections from specific POP3 servers, do the following:
   a. Click **Add** under **Dedicated POP3 Connections**. The Dedicated POP3 Connection window appears.
   b. Type the port IMSS uses for incoming POP3 connections, the POP3 server IP address, and the POP3 server port number.
   c. Click **OK**.
   d. To modify an existing connection, click the connection name.

5. Under **Message Text**, modify the message that IMSS sends to users if email messages that they are trying to receive trigger a filter and are quarantined or deleted.
6. Click **Save**.

Note: The incoming port on your scanners must be idle or the IMSS daemon might not function properly.

Configuring POP3 generic services

For a generic POP3 service, the POP3 client logs on using the USER command and specifies the actual POP3 server and optional port number along with the user's name using the UserServerSeparator character to separate the values.

Example 1: To connect user "User1" to server "Server1", and the UserServerSeparator character is "#", the client issues the following USER command:

USER User1#Server1

Example 2: To connect to port 2000 on Server1, the following command is used:

USER User1#Server1#2000

Note: If you do not specify a port number, IMSS uses the default value of 110.

The following example shows how to configure generic POP3 settings for Outlook:

1. Specify the POP3 server address with IMSS scanner IP 192.168.11.147.
2. Type user name `test123#192.168.11.252`.
3. Set POP3 port to 110.

Configuring POP3 dedicated services

For a POP3 dedicated service, the POP3 service always connects to a specific POP3 server. IMSS uses this service for a POP3 logon and for any type of logon using the AUTH command. For this service, a separate port on the proxy has to be set up for each specific POP3 server that any client might want to connect to.

The following example shows how to configure dedicated POP3 settings in Outlook:

1. Specify the POP3 server address with IMSS scanner IP 192.168.11.147.
2. Type user name `test123`.
3. Set the POP3 port to 1100, which is the port that the IMSS dedicated POP3 service is listening on.

Configuring Database Settings

To configure database settings:

1. Choose **Administration > IMSS Configuration > Connections**. The Components tab displays by default.
2. Click the **Database** tab. The IMSS admin database type, database server name or IP address, and username appear at the top of the table.
3. To register an EUQ database to IMSS, click **Register** under **EUQ Database**.

Note: You must use the installer to install the EUQ database, which then registers it to IMSS automatically.

---

4. Type the EUQ database server FQDN or IP address, port number, administrator username and password.
5. Click **OK**.
6. To modify an existing database, click the database name.
7. To unregister an existing database from IMSS, select the checkbox next to a database, and then click **Un-register**.

Note: You can re-add the database at another time. Unregistering the database does not delete or otherwise affect the actual database server; IMSS just stops using it.

Configuring TMCM Settings

To use Trend Micro Control Manager (TMCM) 5.0 with Patch 3 or above to manage IMSS, enable the Control Manager/MCP agent on the IMSS server and configure Control Manager server settings. If a proxy server is between the Control Manager

server and IMSS, configure proxy settings. If a firewall is between the Control Manager server and IMSS, configure port forwarding to work with the firewall's port-forwarding functionality.

To configure Control Manager settings:

1. Choose **Administration > IMSS Configuration > Connections**. The **Components** tab displays by default.
2. Click the **TMCM Server** tab.
3. Select the **Enable TMCM Agent** check box.
4. Next to **Server**, type the Control Manager IP address or FQDN.
5. Next to **Communication protocol**, select HTTP or HTTPS and type the corresponding port number. The default port number for HTTP access is 80, and the default port number for HTTPS is 443.
6. Under **Web server authentication**, type the access credentials to access the Control Manager Web server.
7. Select **Enable proxy** under Proxy Settings.
8. Next to **Proxy Type**, select the protocol the proxy server uses: **HTTP**, **SOCKS4**, or **SOCKS5**.
9. Type the proxy server FQDN or IP address, port number, and the username and password.
10. Click **Save**.

    If you are using the Configuration Wizard, click **Next**.

    If you enabled the agent, it will soon register to the Control Manager server. If you disabled the agent, IMSS will soon log off from the Control Manager server. Verify the change on the Control Manager management console.

    For additional information about Control Manager, see your Control Manager documentation.

To unregister from Control Manager:

1. Choose **Administration > IMSS Configuration > Connections**. The **Components** tab displays by default.
2. Click the **TMCM Server** tab.
3. Click the **Un-register All Agents** button.

Managing Product Licenses

IMSS can use the following components:

- **Antivirus and Content Filter:** Basic scanning and filtering functionality. You can think of this product as the IMSS program itself.
- **Spam Prevention Solution (SPS):** A built-in filter that helps IMSS identify content typically found in spam.
- **IP Filtering Service:** Automatically blocks known spam senders. IP Filtering includes the following:
  - **ERS:** Trend Micro Email Reputation Services (ERS) are designed to be used to identify and block spam before it enters a computer network by routing Internet Protocol (IP) addresses of incoming mail connections to Trend Micro Web reputation server for verification against extensive reputation databases.
  - **IP Profiler:** IP Profiler allows you to configure threshold settings and determine the action IMSS performs when it detects any of the four potential Internet threats:
    - **Spam:** Email with unwanted advertising content.
    - **Viruses:** Various virus threats, including Trojan programs.
    - **Directory Harvest Attack (DHA):** A method spammers use to add your user's email addresses to spam databases.
    - **Bounced Mail:** Email messages returned to the sender because the messages were sent with the sender's domain in the sender address.

You can activate IMSS products through the Web management console. If a product license expires, you must renew the license, obtain a new Activation Code, and specify the code through the Web management console. If the product remains inactive, its features are disabled.

Viewing Your Product Licenses

To view your existing licenses:

1. Choose **Administration > Product Licenses**. A brief summary of each license appears:
   - **Product**
   - **Version**

- **Full:** Indicates that you have purchased the full licensed product.
- **Evaluation:** Indicates that you are using an evaluation product that expires after an elapsed time. The evaluation period varies according to the Activation Code you have obtained.

  Fourteen (14) days prior to the expiration of the evaluation period, you will see a warning message on the Web management console.

  To continue using IMSS to protect your network after the evaluation period, purchase a licensed version of IMSS and specify the new Activation Code.

- **Activation Code:** A 31 alphanumeric character code in the format **`xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx`**. Trend Micro will send you an Activation Code by email when you register a product online. You can then copy and paste this Activation Code on the Product License page.
- **Seats:** The number of endpoints/servers the license supports.
- **Status:** Indicates whether the product has expired or has been activated.
- **Maintenance expiration:** The date when you will no longer be able to download the latest scan engine and virus pattern files from the Trend Micro ActiveUpdate server. To ensure that your network is protected against the latest Web threats, contact your sales representative to renew your license.

2. For the license you want to view, click **View detailed license online**.
3. To check the status of your license agreement on the Trend Micro Web site, click **Check Status Online**.

Renewing or Activating a License

There are two ways to renew a license:

- **Obtain a new Activation Code:** Contact your sales representative to obtain a new Activation Code, and then specify the code on the Product Licenses screen.
- **Extend the life of an existing Activation Code:** Contact your sales representative to extend the lifetime of your Activation Code, and then either manually update the license status or wait until IMSS automatically updates it.

To renew using a new Activation Code:

1. Choose **Administration > Product Licenses**. A brief summary of each license appears.
2. Next to **Activation Code**, click **Enter a new code**. The Enter a New Code screen appears.
3. Next to **New Activation Code**, type the new code.
4. Click **Activate**. The Web management console might access the Trend Micro Web site to activate the license. If you are unable to reach the Trend Micro Web site, verify your network settings and try again.

To renew using an existing Activation Code:

1. Choose **Administration > Product Licenses**. A brief summary of each license appears.
2. For the license you want to renew, click **View detailed license online**.
3. Click **Check Status Online**. The Web management console accesses the Trend Micro Web site to activate the license. If you are unable to reach the Trend Micro Web site, verify your network settings and try again.

90, 60, 30, and 0 days before the expiration of the current license, and every day after the expiration of the current license, IMSS will automatically check the status of your license and update it if you have extended the valid period.

Tip: You can wait for IMSS to update the license status automatically. However, Trend Micro recommends that you manually update it as soon as you extend the lifetime of the Activation Code.

Activating Products

If you do not have an Activation Code, use the Registration Key that came with your product to register online.

Activate products from one of the following screens:

- From step 6 of the Configuration Wizard.
- From **Administration > Product Licenses**

To activate from step 6 of the Configuration Wizard:

1. If you do not have an Activation Code, click **Register Online**. Upon successful registration, Trend Micro will send you the Activation Code through email.
2. Type the Activation Code to activate any of the following:
   - Trend Micro Antivirus and Content Filter
   - Spam Prevention Solution
3. Click **Next**.

Note: The Activation Code comes in the format xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx.

To activate from Administration > Product Licenses:

1. Choose **Administration > Product Licenses**. A brief summary of each license appears.
2. Next to Activation Code, click **Enter a new code**. The Enter a New Code screen appears.
3. Next to New Activation Code, type the new code.
4. Click **Activate**. The Web console may access the Trend Micro Web site to activate the license. If you are unable to reach the Trend Micro Web site, verify your network settings and try again.

Chapter 8

Troubleshooting, FAQ, and Support Information

This chapter explains how to troubleshoot common IMSS issues, search the Trend Micro Knowledge Base, and contact support.

Topics include:

Troubleshooting

Table 8-1 shows common troubleshooting issues that you might encounter when installing, configuring, or administering IMSS. Read the solutions below. If you have additional problems, check the Trend Micro Knowledge Base.

For troubleshooting and FAQ information pertaining to the deployment of IMSS, refer to the *IMSS Installation Guide*.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
General	
Unable to access the Web console or other components.	The target port is not in the firewall approved list. Open the ports as shown in Table 8-2 on page 8-12 in the firewall. If you are unable to access the Web console, do the following: 1. Start the database process, `dbctl.sh`, before starting the Central Controller process, `S99ADMINUI`. 2. If you are still unable to access the Web console, restart the Central Controller process, `S99ADMINUI`. For more details, refer to Using IMSS Scripts on page A-2.
No access to the Web console	The Web console URL is not a trusted site in Internet Explorer. Add the URL to the trusted sites.
The imssps daemon is running but refusing connections.	If the imssps daemon is running, the policy service is working. Check the connection between the policy service and scanner service and verify your LDAP settings.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Unable to activate products (Antivirus/eManager, SPS, ERS, IP Filtering) or update components	To activate ERS, IMSS needs to connect to Trend Micro. This process requires an HTTP query with a valid DNS setting. Therefore, if a DNS server is not available or has connection problems, activation cannot occur. **To verify your DNS server settings**: 1. Use the following command: nslookup licenseupdate.trendmicro.com The command should return the IP address of your IMSS server. If a proxy server is required to connect to the Internet, verify your proxy settings to ensure the HTTP request reaches http://licenseupdate.trendmicro.com. **To verify your proxy settings from the Web console:** 1. Click **Administration > Updates**. The Schedule tab displays by default. 2. Click the **Source** tab. 3. Configure the proxy settings. 4. Click **Save**.
Email notifications do not display properly.	If your computer is running a non-English operating system and the notification message was not written in English, it may appear distorted. Modify the character set through the Web console. **To modify the character set:** 1. On the Web console menu, choose **Administration > Notifications > Delivery Settings**. 2. Next to **Preferred Charset**, select the character set in which the messages will be encoded.
Cannot query message logs in IMSS.	IMSS scanner records the log with local time. To query message logs, synchronize the date/time on all computers with IMSS.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Server displays as disconnected in the Summary screen.	A managed server could become disconnected for any of the following reasons: • The scanner was removed from your network. • The IMSS manager service has stopped. • Network connection issue has occurred. Check your firewall settings for the Manager Service listening port. Click **Administration > IMSS Configuration > Connections > Components > IMSS Manager Port.**
When viewing detailed information for quarantined or archived email, attachment information is sometimes not available.	IMSS records attachment information only when the triggered rule is for an attachment. Check the reason why IMSS quarantined the email.
IMSS does not receive email.	1. Check if the IMSS scanner service is running. 2. Check if a different application is using the required port. Free up port 25.
Services are not running normally.	The database has not been started or the database was started after the IMSS services started. Restart all IMSS services.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
After enabling Web reputation, the scan time for messages increases significantly.	Web reputation needs to query the Trend Micro Web reputation servers.Verify the HTTP connectivity from the IMSS scanner to the external network. If it requires a proxy server to connect to the Internet, configure proxy settings on the Updates Source screen: 1. Click **Administration > Updates > Source**. The Updates Source screen appears. 2. Select the **Use a proxy server for pattern, engine, and license updates** check box. 3. Configure the proxy settings. 4. Click **Save**. For Web reputation issues, check the wrsagent.* files under the /opt/trend/imss/log folder.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
End-User Quarantine Issues	
Unable to access the EUQ Web console	Do the following: 1. Verify that you are using the correct URL and port number. To view the console from another computer on the network, type the following URLs: • Primary EUQ service: `https://<target server IP address>:8447` • Secondary EUQ service: `https://<target server IP address>:8446` 2. Verify that the system time of each EUQ service on your network is synchronized. The first instance of the EUQ service, the primary EUQ service, runs Apache Web Server (httpd) while listening on port 8447 (HTTPS). This Web Server serves as a connection point for the EUQ clients and for load balancing for all EUQ services. If the Apache server is not up and running, users will not be able to access the EUQ console from the normal IP address: `https://{Primary EUQ Service IP address}:8447/.`

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Users are unable to log on to EUQ Web console	Do the following: 1. On the LDAP server, verify that the user accounts are in the correct group. Only user accounts in the approved group can access EUQ. 2. Verify LDAP and User Quarantine Access settings through the IMSS Web console: a. Choose **Administration > IMSS Configuration > Connections > LDAP** from the menu. b. Verify all settings, especially the LDAP type and server information. If you are using Kerberos authentication, ensure that the time for all IMSS computers and the LDAP server is synchronized. c. Choose **Administration > User Quarantine Access** from the menu. d. Enable User Quarantine Access. e. Verify that the correct LDAP groups appear under Selected Groups and that the user account belongs to the selected groups. 3. Verify that users are using the correct logon name and password. For more information, see Logon Name Format on page 1-21. 4. If the issue persists even after verifying the above settings, do the following: a. Choose **Logs > Settings** from the menu. b. Set the application log level to **Debug**. c. Choose **Summary** from the menu. From the **System** tab, restart the Web EUQ service. d. Request the user to try logging on to the EUQ Web console again. e. Send the log file `imssuieuq.yyyymmdd` located in `/opt/trend/imss/logs` to Trend Micro's technical support.
The EUQ Web digest does not display quarantined email information correctly	Verify that the correct character set is selected: 1. Choose **Administration > Notifications > Delivery Settings**. 2. Next to **Preferred charset**, choose the character set that will properly display the digest information.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Some quarantined email messages are not appearing on the EUQ Web console	On the EUQ Web console, users can only access the quarantined email messages if the administrator configures EUQ to allow access. **To make Quarantine Areas visible to end users:** 1. Click **Quarantine & Archive > Settings**. 2. Click the link of the Quarantine Area that you want to synchronize to EUQ. 3. Select the **Sync mails quarantined by content filter to EUQ database (for this area only)** check box. After enabling this option, all non-malicious messages (messages that do not trigger antivirus rules, anti-phishing conditions, or Web reputation) quarantined in this area synchronize with the EUQ database. This allows end users to view and manage the messages from the EUQ Web console. End users cannot access malicious messages.
Cannot enable LDAP with Kerberos authentication.	Kerberos protocol requires time synchronization between the Kerberos server and IMSS. Synchronize the date/time for all computers with IMSS.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
IP Filtering Issues	
FoxProxy cannot start up	There are several reasons why FoxProxy might not start. To find out the reason, view the IP Profiler logs. To view IP Profiler logs: 1. Go to the directory where IP Profiler is installed (by default: `/opt/trend/ipprofiler/config`). 2. Open `foxproxy.ini`. 3. Change the value for `log_level` to **4**. 4. Restart FoxProxy by typing the following: `/opt/trend/ipprofiler/script/foxproxyd restart` 5. Open the log file by typing the following: `/opt/trend/ipprofiler/logs/foxproxy-general.****`
Unable to connect to FoxProxy	Verify that FoxProxy is running and that it binds on port 25.
FoxProxy processes email messages slowly	When FoxProxy receives email, it performs a DNS query on FoxDNS. If Bind is not running, FoxProxy continues to wait until the DNS query times out. Verify that the bind service is running on the computer where FoxDNS is installed: 1. Type the following command: `ps –ef | grep named` 2. Start the service if it is not running.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Unable to view connections that FoxProxy is blocking	Every five (5) minutes, FoxProxy sends information about blocked connections to the IMSS server. Wait for at least five minutes before viewing the connection information. To change this time value: 1. Open `foxproxy.ini`. 2. Modify the value for `report_send_interval`. 3. Restart FoxProxy by typing the following: /opt/trend/ipprofiler/script/foxproxyd restart
FoxDNS is not functioning	Verify that the BIND service is running: 1. Type the following command: `ps -ef | grep named` 2. Start the service if it is not running.

No IP Profiler log information exists	The following IP Profiler-related log files are in the IMSS admin database:
	• `foxmsg.****`
	• `foxnullmsg.****`
	• `foxreport.****`
	Verify that the log files exist:
	1. Go to the log directory where IMSS is installed (by default: `/opt/trend/imss/log/`).
	2. If the files are not present, use the following command to check if imssmgr is running:
	`ps -ef | grep imssmgr`
	3. Check if FoxProxy is running:
	`ps -ef |grep foxproxy`
	4. Verify that IP Profiler is enabled. In the table 't_foxhuntersetting', the following should exist:
	`record: 'Type' = 1` and `'enable' = TRUE`

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
ERS does not work after being enabled from the Web console.	ERS may not work due to the following reasons: • Spam Prevention Solution (SPS) was not activated. ERS shares the same Activation Code with SPS. If SPS has not been activated, activate SPS and then activate ERS. • The computer on which the scanning service is installed cannot access the Internet. MTA cannot get a response for the DNS query for Activation Code validation. Confirm that the computer where the scanner service is installed has access to the Internet. Activate SPS and confirm that the computer with SPS installed can access the Internet.
The MTA settings on the **SMTP Routing** Web console screen are not being written into the Postfix configuration files	By default, the settings on the SMTP routing screen will not be automatically applied to Postfix on each scanner. To apply the settings to all scanners: 1. Click **Administration > IMSS Configuration > SMTP Routing**. The SMTP Routing screen appears. 2. Select the **Apply settings to all scanners** check box. 3. Click Save. After a few minutes, the IMSS manager process on each scanner synchronizes the settings to Postfix. To restart the IMSS manager immediately, use the command: /opt/trend/imss/script/S99MANAGER restart If the process above does not work, check the local configuration file /opt/trend/imss/config/imss.ini to verify the enable_postset_thd key is set to "yes" or is blank.
IP profiler does not block IP addresses in the Blocked List.	The changes require about one (1) minute to take effect. Wait one (1) minute before checking the list again.

TABLE 8-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Blocked IP address does not display in the Overview page	The Overview page displays the top 10 blocked IP addresses by type for the last 24 uninterrupted hours. For example, at 16:12 today the Overview page displays data from 16:00 yesterday to 16:00 today. View the Overview page after an hour.

IMSS Ports

TABLE 8-2. IMSS Ports

Module	Port	Description
Admin UI	8445	Tomcat listening port (HTTPS)
Bind	53	Name-domain server
EUQ UI	8009	Tomcat AJP (load balance) port
EUQ UI	8446	Tomcat listening port
EUQ UI	8447	Load balancer
Manager	15505	SOAP server
Policy Server	5060	SOAP listening port
Scanner	110	POP3 listening port

Frequently Asked Questions

Postfix MTA Settings

If I deploy multiple scanners with Postfix, how can I manage these Postfix instances centrally? Can I make an exception on the settings for some Postfix instances separately?

To control all the Postfix computers from the Web management console, enable the "**Apply settings to all scanners**" option. Choose **Administrator** > **SMTP Routing** > **SMTP** from the menu.

To make an exception for some Postfix settings, search for the key "`detach_key_postfix`" in `imss.ini`, and add the keys that you do not want to apply from the Web management console. For example:

```
detach_key_postfix=smtpd_use_tls:queue_directory:{Parameter1
:{Parameter2}:…::{Parameter n}
```

The parameters above will not be overwritten by any settings that you configure through the Web console. You can modify `main.cf` manually.

Note: "{Parameter1:{Parameter2}:…::{Parameter n}" means you can use one or more parameters by separating them using colons.

You can find the parameter names in the table `tb_postfixconfig` from the database, under the column `fieldname`.

WARNING! **Use extreme caution when modifying the configuration file.**

IMSS Components

Can I move the Central Controller from one computer to another?

Yes. First, run the IMSS installation script to uninstall the Central Controller from the computer. Next, run the IMSS installation script and install the Central Controller on the other computer.

How can I set up and maintain the database?

The following commands can help you maintain the database:

- pg_dump –d imss –U sa > YYMMDD.HHMMSS.backup: Back up the database.
- psql -Usa -d imss < ./YYMMDD.HHMMSS.backup: Retrieve the latest data if errors occur.
- `vacuum`: Clean up the database on tables that are frequently accessed or on tables that have large amounts of data. Use this command when email traffic is low or when the device is not connected to your network.
- `vacuumfull`: Clean up the entire database when the database is not being heavily utilized or when the device is not connected to your network.
- `redirect_stderr= and log_rotate_***=` Turn on these options in `postgresql.conf` to redirect old database log entries to the system log, which is rotatable. You can name the log file to start with a dash "-".

Is IMSS policy service able to work if LDAP is not up and running?

Yes, the policy service still works even if the LDAP server is not up and running.

Following are three scenarios of such a situation.

- IMSS continues to work as usual.
  - If the LDAP server is active but the port of the LDAP server is inaccessible.
  - If the policy server has the non-expired cache of the LDAP user or group.
- IMSS will spend about one minute to perform each rule query. The policy server will bypass the LDAP-related rules and continue to process other rules. This may slow down message scanning and result in long mail queues.
  - If the LDAP server is down or the port of the LDAP server is inaccessible.

Email Reputation Services

How do I configure Email Reputation Services (ERS) to not block certain IP addresses or domains?

Add the IP addresses / domains to the ERS approved list by doing the following:

- Log on to the Web console.
- Click **IP Filtering > Approved List**.

- Add the IP addresses or domains that you do not want blocked to the Approved List.

Note: If the domain cannot be resolved by the DNS service, the domain will not work in the approved list.

How do I specify the Activation Code for ERS?

You can provide the Activation Code during installation, or you can modify it after installation.

To modify the Activation Code, edit the Postfix configuration files located in the same computer as ERS. These files are `main.cf`, `imss_rbl_reply`, and `imss_rbl_reply.user`.

Note: The `imss_rbl_reply.user` file may not exist. If it exists, modify it. Otherwise, you can omit it.

After installing ERS, you should see similar contents in the three configuration files as follows:

- **main.cf**

  smtpd_client_restrictions = reject_rbl_client APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com,reject_rbl_client APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com

- **imss_rbl_reply**

  APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com 450 Service temporarily unavailable; $rbl_class [$rbl_what] blocked using Trend Micro Email Reputation Service. See http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?; $rbl_reason}

  APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 550 Service unavailable; $rbl_class [$rbl_what] blocked using Trend Micro RBL+. See http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?; $rbl_reason}

- **imss_rbl_reply.user**

APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com 450 error message; $rbl_class [$rbl_what] blocked using Trend Micro Email Reputation Service. See http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?; $rbl_reason}

"APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 450 error message; $rbl_class [$rbl_what] blocked using Trend Micro RBL+. See http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?; $rbl_reason}

Replace the old Activation Code with your new Activation Code in these three files. The old Activation Code shown in the above examples is APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.

Note: You do not need to type the dash '-' for the Activation Code.

After editing the configuration files, restart Postfix using the commands:

postfix stop

postfix start

IP Profiler

How can I purge the FoxProxy log?

A log purge program exists in the IP Profiler installation directory (by default: `/opt/trend/ipprofiler/bin/TmFoxPurgeLog`).

The settings about log purge function are in the configuration file `foxproxy.ini`. The keys are as follows:

- log_purge
- log_purge_unit
- log_purge_num

Which process monitors FoxProxy's status? Which process rescues it when it shuts down?

FoxProxy is a multiple-process program. The main process only monitors child processes. If child processes are stopped, the main process rescues them. But if the main process is stopped, the child processes cannot be rescued.

If you are experiencing any problems with FoxProxy, verify that the main process is running.

Which process/component performs DNS queries?

The DNS queries are performed directly by FoxProxy.

The installer gives users the option to install a DNS server on the Central Controller, if the installer does not detect any existing DNS server. When you install IP Profiler, the installer will prompt you for the IP address of the Central Controller.

Why is the domain name of an IP address that was added to the blocked/approved list always N/A?

IMSS does not determine the domain name of an IP address that was added to the blocked/approved list (IMSS does resolve the IP address of an added domain name).

Why does the IP Filtering Suspicious IP screen also display the connection information of blocked IP addresses?

The **IP Filtering > Suspicious IP** screen shows all information for successful connections. Therefore, although an IP address is now in the blocked list, the previous connections for this IP address, which have not been blocked, are shown.

How does IP Profiler process email?

The IP Filter decides if the source IP address is a safe IP address. IMSS scanner service queries matched policies from the IMSS policy service. The policies are applied to the email in the required order. If a policy specifies that an email should be quarantined, deleted or delivered, then the action is taken and the remaining policies are not applied.

Can the IP Profiler use an existing BIND server?

Yes. The IP profiler requires a BIND server. When a user installs IMSS, if a BIND server is already present on the computer, the IP profiler will use this BIND server. If a BIND server is not present, then IMSS installs a new BIND server.

When does IMSS 7.1 send an email to "`Foxhunter_proxy@domain`"?

IMSS will send an email to "`Foxhunter_proxy@domain`" under the following three conditions:

- When FoxProxy receives an "Incomplete" message.
- When FoxProxy receives a "Null" message.

- When FoxProxy rejects a connection, it will send a statistics mail every 5 minutes. You can configure the time interval by modifying the `report_send_interval` (unit in seconds) setting in `foxproxy.ini`.

Is the LDAP service mandatory for analyzing whether an incoming traffic is a form of DHA attack?

Technically, LDAP service is not a must-have. The DHA rule of IMSS 7.1 relies on the result returned from Postfix, which in turn passes the result to FoxProxy, a sub-module of IP Profiler, for analysis. The LDAP server is just one of the many means by which Postfix checks for the existence of a recipient's mailbox.

Quarantine and Archive

Can I use special characters to perform queries?

Yes, you can use the following special characters to perform queries:

- **Asterisk (*):** Used as a wildcard character to search for zero or more characters. You can use asterisk (*) to search for email addresses or file names.

  To search for email addresses, see the following examples:

  ***:** Valid representation of all email addresses.

  `*@domain.tld, name@*.tld`: Valid representation of the whole name or the domain (not the top level domain (TLD)).

  `*@*.tld`: Valid representation of both the name and the domain (not the TLD).

  To search for file names, see the following examples:

  `*.*`: Valid representation of all files.

  `*.extension` : Valid representation of all files of a certain extension.

  `name.*`: Valid representation of files with a specific name but of any extension.

- **Semicolon (;):** Used as a separator when searching for multiple recipients or attachments.

Why is there a quarantined message without a message ID when the user views message details?

IMSS reprocesses notification email messages for security reasons. Therefore, if a notification email message was quarantined due to a policy violation, then the notification email message generated by IMSS would not have a message ID.

End-User Quarantine

If I am using Kerberos, why are users unable to log on to the EUQ console with a short name: "domain\user_name"?

Kerberos servers cannot accept user names in the format: `Domain\user_name`. Kerberos requires the format `user_name@domain.xxx`

If I installed Microsoft Exchange Server, and have set multiple mail addresses for each user, how do I enable EUQ to check multiple mail addresses for one user?

If you installed one Microsoft Exchange Server together with the Active Directory, you can do the following:

a. Open the table `tb_global_setting` in IMSS administrator database and replace the value of `LDAP-->mail_attr` from "mail" to "proxyAddresses".

b. Restart all IMSS services.

How do I send a non-English EUQ digest?

Do the following:

a. In the Web console, click **Administration > Notifications >Web EUQ Digest**.

The Web EUQ Digest screen appears. Type the EUQ subject or content in the non-English language.

b. Click **Administration > Notifications > Delivery Settings**.

The Delivery Settings screen appears. Select any non-English language as the Preferred character set.

How can I speed up my LDAP access if the LDAP server is Active Directory?

There are two methods to speed up your access. The method you use depends on the port number you can use: port 389 or port 3268.

Active Directory uses port 3268 for the Global Catalog. LDAP queries directed to the global catalog are faster because they do not involve referrals to different domain controllers.

Tip: Trend Micro recommends using port 3268 for LDAP queries.

Active Directory uses port 389 for LDAP query. If one item cannot be queried in one domain controller, it uses the LDAP referral mechanism to query another domain controller. Use port 389 if your company has only one domain or if port 3268 is unavailable.

To use port 3268 for LDAP queries:

a. Click **Administration >IMSS Configuration > Connections**. The Connections screen appears.

b. Click the **LDAP** tab.

c. Configure the LDAP listening port as 3268.

To use port 389 for LDAP queries:

a. Click **Administration >IMSS Configuration > Connections**. The Connections screen appears.

b. Click the **LDAP** tab.

c. Configure the LDAP listening port as 389.

d. Add the following key into the `imss.ini` file, which is at `$IMSS_HOME\config`.

```
[LDAP-Setting]
DisableAutoChaseReference=yes
```

e. Restart all IMSS services.

What user logon name formats does IMSS support for Active Directory?

Active Directory supports the following logon name formats:

- Example 1: `bob@imsstest.com`

Note: The logon name is not an email address (though it appears as one).

- Example 2 (pre-Windows 2000): `IMSSTEST\bob`

Note: The pre-Windows 2000 format is not supported by Kerberos authentication.

Spam Protection Service

How is the spam catch rate determined?

Specify a threshold value between 3.0 and 10.0 for IMSS to classify an email message as spam. A high threshold value means that a message must be very "spam-like" to be classified as spam (this decreases the spam catch rate but reduces the likelihood of false positives). A lower threshold value means that a message only needs to be slightly "spam-like" to be classified as spam (this increases the spam catch rate and may lead to more false positives).

ActiveUpdate

How do I roll back a pattern file?

Click the **Rollback** button on the Summary page.

Others

Can the database server be referenced by hostname?

Yes. You can specify the IP or hostname.

Can the server IP address be changed?

Yes.

To change the server IP address:

a. Stop all IMSS services by running the `$IMSS_Home/imss/script/imssstop.sh stop` command or stop the services individually.

For more information on IMSS scripts, see Using IMSS Scripts on page A-2.

b. Change the server IP address.

c. Start the database service if it is installed on this server. If IMSS installed the database use the following command:

```
$IMSS_Home/imss/script/dbctl.sh start
```

d. Change the IP address in the odbc.ini and euqodbc.ini files. The files are located in the IMSS configuration folder: $IMSS_Home/imss/config/.

e. Change the database URL and user name/password in `%IMSS_HOME%/UI/adminUI/ROOT/WEB-INF/struts-config-common.xml`

f. Change the following database data:

- `tb_component_list`: Specify the computer name and all scanner IP addresses.
- `tb_euq_db_info`: Specify the EUQ database computer settings.
- `tb_global_setting`: In section [cmagent] name [ConfigUrl], change the Web console URL.

g. Start all IMSS services with the following command:

```
$IMSS_Home/imss/script/imssstart.sh
```

How does IMSS process a partial email message?

The key `BypassMessagePartial` in the IMSS configuration file `imss.ini` controls how IMSS processes partial email messages.

IMSS rejects partial email messages as a malformed message if `BypassMessagePartial=no` in the `imss.ini` file.

If the key is set to `yes` (default setting), IMSS will bypass partial email messages.

What file format can IMSS import when configuring policy settings?

IMSS can only import .txt file containing only one item per line. Following are examples of how you can import a text file from the Web management console:

a. When specifying the attachment to be scanned

- Click **Policy** > **Policy List** from the menu.
- Click the link of an existing rule to edit a rule.
- Click the **And scanning conditions match** link.
- Click the **Name or extension** link under the Attachment section.
- Select the check box next to **Attachment named**.
- Click **Import**. The imported file should be a text file containing one file name or extension per line.

b. When configuring the spam detection settings

- Click **Policy** > **Policy List** from the menu.
- Click the link of an existing rule to edit a rule.

- Click the **And scanning conditions match** link.
- Click the **Spam detection settings** link.
- Select the check box next to **Approved sender list** or **Blocked sender list**.
- Click **Import**. The imported file should be a text file containing one email address per line.

Why are newly created administrator accounts not able to access the User Quarantine Access, Admin Accounts, and Product License pages?

Only the default IMSS admin account has the permission to access the User Quarantine Access, Admin Accounts, and Product License pages. Custom admin accounts cannot access these pages.

Why are changes to the IMSS configuration settings not applied immediately?

There is a lapse between the time you modify the configuration settings from the Web management console and the time modifications are actually updated on the IMSS server.

Policy settings will be reloaded in no longer than three (3) minutes. If you want the settings to load faster, modify the `policy_server=>dbChangePollIntervalInSecs` setting in the `tb_global_setting` table of the IMSS administrator database as desired.

For other general settings, imssmgr will take no longer than one (1) minute to reload the new settings modified from the Web management console.

Tip: Trend Micro recommends that you do not send mail to IMSS immediately after modifying the configuration settings from the Web management console.

Is there any limit on the maximum number of the following items?

- Senders and recipients for each rule
- Mail addresses in one address group
- Approved/Block Senders for SPS rule

Technically, there is one limitation on the total size of each rule, which is 640KB. The total size includes the rule route (senders/recipients), rule filter (scanning condition), and rule action. Assuming that each email address/LDAP account consists of 20 characters, IMSS can support at least 10,000 senders/recipients for the rule route.

The maximum number of mail addresses for one address group is 10,000.

The maximum number of Approved/Block Senders for SPS rule is 5000.

How can I modify the log paths?

If you want to modify some log paths, locate the following keys in `imss.ini` and change the default settings as desired.

[general]

sys_log_path=/opt/trend/imss/log

event_log_path=/opt/trend/imss/log

policy_evt_log_path=/opt/trend/imss/log

Can IMSS 7.1 configure its own relay restrictions if a third-party upstream server is not installed?

No. IMSS 7.1 cannot configure its own relay restrictions as it does not have its own MTA on the Linux platform. You can only configure relay restrictions using a third-party MTA.

How can I modify the Access Control List (ACL) for the IMSS scanner?

You can modify the following settings in `imss.ini`.

- Add the target IP address to the parameter `smtp_allow_client_ip`.
- Alternatively, disable ACL check by setting `open_to_all_connections=yes`.
- To ensure that other computers are able to connect to the scanner, insert the target IP addresses in the parameter `proxy_smtp_server_ip`.

For more details, refer to the comments in `imss.ini`.

Why are email messages from some senders always received as attachments? Why is the mail body replaced by the disclaimer or stamp?

When the character set of the stamp is different from the character set of the email message content, IMSS will encounter issues inserting the stamp into the message body after scanning the message. In this situation, IMSS will create a new email message, insert the stamp into the message body, and attach the original message. The message content, however, will not be changed.

How can I specify a keyword expression to represent a blank header for matching fields such as "from", "to", or "subject" when creating rules with the content filter?

If you are going to use a regular keyword expression to represent a blank header, Trend Micro recommends that you use "`^(\s)*$`" (without the quotation marks). The expression "`^(\s)*$`" (without the quotation marks) represents a blank header or whitespace characters.

For example, if you want to check if a mail's "**from**" header is blank, you can edit a rule's scanning condition as follows:

a. On the Web management console, click **Policy** > **Policy List**.

b. Click the link for an existing rule to edit the rule.

c. Click **And scanning conditions match**.

d. Click **Header keyword expressions** under the **Content** section.

e. Click **Add** to create a new keyword expression.

f. Add the content as "`^(\s)*$`" (without the quotation marks).

Why does the message size scan condition not work for encrypted messages?

IMSS treats encrypted messages as a special type of message. Most scan conditions do not apply. IMSS requires the use of the encrypted message scan condition to scan or perform actions on encrypted messages.

Using the Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

http://esupport.trendmicro.com

The contents of Knowledge Base are being continuously updated, and new solutions are added daily. If you are unable to find an answer, however, you can describe the problem in email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

Contacting Support

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all of our registered users. Get a list of the worldwide support offices:

http://www.trendmicro.com/support

Get the latest Trend Micro product documentation:

http://www.trendmicro.com/download

In the United States, you can reach the Trend Micro representatives by phone, fax, or email:

Trend Micro, Inc.
10101 North De Anza Blvd.
Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Web address: www.trendmicro.com

Email address: support@trendmicro.com

TrendLabs

TrendLabs^{SM} is the global antivirus research and support center of Trend Micro. It is located on three continents, with a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales services:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Email access to antivirus engineers
- Knowledge Base, the Trend Micro online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

Comprehensive security information is available at the Trend Micro Web site:
`http://www.trendmicro.com/vinfo/`

At the top of the Web console, click the Help drop-down box, then Security Info. Information available:

- List of viruses and malicious mobile code currently "in the wild," or active

- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Security advisories
- Scams and hoaxes
- Joke programs
- Spyware/Grayware
- Phishing Encyclopedia

Staying Up to Date

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to your product. To find out whether there are any patches available, visit the following URL:
`http://www.trendmicro.com/download/`

The Update Center screen displays. Select your product from the links on this screen. Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the installation instructions in the readme.

Sending Suspicious Files to Trend Micro

If you have a file you think is infected but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us. For more information, refer to the following site:

http://subwiz.trendmicro.com/subwiz

Include in the message text a brief description of the symptoms you are experiencing. The team of antivirus engineers will analyze the file to identify and characterize any virus(es) it may contain, usually on the same day it is received.

You can also send an email to: **virusresponse@trendmicro.com**, and specify "Phish or Disease Vector" as the Subject.

Appendix A

IMSS Scripts

This appendix provides you with a list of IMSS scripts and their respective parameters that you can invoke from the command line.

Topics include:

Using IMSS Scripts

IMSS scripts provide a convenient and alternative means of performing administrative tasks from the command line.

See *Table A-1* for a list of the scripts, their respective parameters and the functions they perform.

All scripts listed in the table are located in `/$IMSS_Home/imss/script`, except `foxproxyd`, which is located in `/$IMSS_Home/ipprofiler/script` .

TABLE A-1. IMSS scripts

SCRIPTS	PARAMETERS	DESCRIPTIONS
foxproxyd	start / stop / restart	IP Profiler service
dbctl.sh	start / stop / restart	Postgres database service
imsstop.sh		Forces all IMSS services to stop.
postfixctl.sh	start / stop / reload / restart	Postfix daemon
regippro.sh	reg / unreg	Register or unregister IP Profiler to or from the admin database.
S99ADMINUI	start / stop / restart	Central Controller
S99CLEANEUQ		Removes expired quarantined data from the EUQ and admin databases as configured under the **Administration** > **User Quarantine Access** area of the Web management console.
S99CLEANEXPIRE		Removes expired quarantined and archived data from the EUQ and admin databases as configured under the **Quarantine & Archive** > **Settings** area of the Web management console.
S99CMAGENT	start / stop / restart	CMAgent service

TABLE A-1. IMSS scripts

SCRIPTS	PARAMETERS	DESCRIPTIONS
S99DIGEST		Sends the EUQ digest message
S99EUQ	start / stop / restart	EUQ service
S99FOXDNS	start / stop / restart	Foxdns service
S99IMSS	start / stop / restart	IMSS scanner service
S99MANAGER	start / stop / restart	Manager service
S99MONITOR	start / stop / restart	Manager monitor service
S99POLICY	start / stop / restart	Policy service
S99REPORT	[option] start / stop / restart [option]: • **-s**: generates centralized reports (covers all one-time and scheduled reports configured on the Web management console) • **-h**: generates hourly individual traffic data • **-t**: generates hourly traffic data • **-d**: performs database log maintenance	Used by S99SCHEDULED to generate related reports. **Note:** Do not run this script on its own.
S99UPDATE	start / stop / restart	Used by S99SCHEDULED to run the scheduled update. **Note:** Do not run this script on its own.
S99SCHEDULED	start / stop	Starts the scheduled task.
forceUpdate.sh	DBDSN username password	Notifies the policy server to reload the policy settings
euqtrans	all / approved sender	Transfers EUQ database data or approved senders
imssstart.sh		Start all IMSS services

TABLE A-1. IMSS scripts

SCRIPTS	PARAMETERS	DESCRIPTIONS
S99WRSAGENT	start / stop / restart	WRS agent service
db_maintain.sh	{vacuum|reindex|analyze|all} [vacuum] - Vacuum admin db and all euq db. [reindex] - Reindex admin db and all euq db. [analyze] - Analyze admin db and all euq db. [all] - Vacuum && Reindex && Analyze.	Used by S99SCHEDULED to the database maintenance. **Note:** Do not run this script on its own.

Appendix B

Default Directory Locations

This appendix provides information on the default directory locations that IMSS uses for mail processing.

Topics include:

Default Mail Queues

Table B-1 shows the various mail directories that store the mail messages managed by IMSS.

TABLE B-1. Default IMSS Mail Locations

QUEUES FOR REGULAR MAILS	QUEUES FOR LARGE MAILS	DESCRIPTIONS
queue_malform=/opt/trend/imss/queue/malform		Stores malformed messages.
queue_archive=/opt/trend/imss/queue/archive		Stores archived messages.
queue_quarantine=/opt/trend/imss/queue/quarantine		Stores quarantined messages.
queue_notify=	queue_notify_big=/opt/trend/imss/queue/notifybig	Stores notification messages.
queue_postpone=/opt/trend/imss/queue/postpone	queue_postpone_big=/opt/trend/imss/queue/postponebig	Stores postponed messages.
queue_deliver=/opt/trend/imss/queue/deliver	queue_deliver_big=/opt/trend/imss/queue/deliverbig	Stores messages for final delivery.
queue_reprocess=/opt/trend/imss/queue/reprocess	queue_reprocess_big=/opt/trend/imss/queue/reprocess-big	Stores messages pending reprocessing.
queue_handoff=/opt/trend/imss/queue/handoff	queue_handoff_big=/opt/trend/imss/queue/handoffbig	Stores messages pending handoff.

TABLE B-1. Default IMSS Mail Locations

QUEUES FOR REGULAR MAILS	QUEUES FOR LARGE MAILS	DESCRIPTIONS
queue_undeliverable=/opt/trend/imss/queue/undeliver-able		Stores undeliverable messages.
queue_unnotify=/opt/trend/imss/queue/unnotify		Stores undeliverable notification messages.

eManager, Virus and Program Logs

Many modules in IMSS write log information for troubleshooting purposes to the following folder:

/opt/trend/imss/log

Temporary Folder

IMSS stores all application-generated temporary files in the temporary folder: `/opt/trend/imss/temp/`

Note: This directory is not configurable.

Notification Pickup Folder

IMSS stores all notification messages, picks them up from the following folders, and then delivers them to a specified SMTP notification server:

/opt/trend/imss/queue/notify/

and

/opt/trend/imss/queue/notifybig

To configure the SMTP notification server:

Choose **Administration** > **Notifications** > **Delivery Settings** from the menu.

Note: The queue_notify_big queue is for large mail messages.

Index

T

U

V

W